Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 17-Mar-1998
Dist. : 19-Mar-1998

Or. Eng.

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

Group of Experts on Information Security and Privacy

REVIEW OF THE 1992 GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

63278

Unclassified DSTI/ICCP/REG(97)2/FINAL Or. Eng.

REVIEW OF THE 1992 GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

This report was prepared by the Secretariat with the assistance of a consultant, Dr. Ted Humphreys, XiSEC Consultants LTD, UK to address the responses to the questionnaire to the Member countries for a review of the 1992 OECD Guidelines on Security of Information Systems. It was then approved by the Group of Experts on Security, Privacy and Intellectual Property Protection in the Global Information Infrastructure (since October 1997 renamed the Group of Experts on Information Security and Privacy, referred to as "the Group of Experts") under the aegis of the Committee for Information, Computer and Communications Policy.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 5

PART 1: SUMMARY OF RESPONSES 7
1.1 Introduction 7
1.2 Overall Summary 8
PART 2: RECENT ISSUES, CONCLUSIONS AND FUTURE ACTION 20
2.1 Recent Developments and Issues 20
2.2 Conclusions and Future Actions 21

ANNEX: INDIVIDUAL SUMMARIES 25

EXECUTIVE SUMMARY

The OECD Guidelines for the Security of Information Systems[1] were adopted in 1992. The Recommendation of the Council concerning these Guidelines suggests they be reviewed every 5 years with a view to improving international co-operation on issues relating to the security of information systems. The review process was conducted by means of a questionnaire issued to Member countries.

This report addresses the responses to this questionnaire. In Part 1 of this report an overall summary is provided of the responses of OECD Member countries to the questionnaire. Part 2 of this report provides a commentary on recent issues based largely on these responses but also taking views and facts from other published sources. It also provides some conclusions and suggested future actions based on the responses and conclusions. An annex to this report gives a summary of each of the individual responses.

The following are some of the main conclusions given in Part 2 of this report as derived from the responses received.

Since the adoption of the 1992 OECD Security Guidelines a continuing programme of activities has been undertaken by Member countries to implement and promote these Guidelines. These activities have resulted in the enactment of legislation, development of standards, technical and management criteria and various other measures. It has also led to the initiation and participation in a number of projects and studies at the national, regional and international levels. Furthermore, the Guidelines have been promoted and referenced in conferences, publications and recommendations in both the public and private sectors. (See Part 1, Q1-Q3, Q10 and Part 2, clause 2.2.1).

Over the intervening period, since the publication of the 1992 Guidelines, various other security issues have emerged that need to be addressed (see Part 2, clause 2.1), e.g. with regard to the increased connectivity between information systems, the related broadening scope of communication systems and the development and use of the GII/GIS. In addition, there are a number of challenges facing the legal system that also need to be addressed. The Member country responses have indicated a number of these problems, issues and challenges (see Part 1, Q4-Q7, and Part 2, clauses 2.2.2 and 2.2.3). Awareness of the issues and the need for security measures is increasing in both the public and private sectors. However, there is still room for improvement in a number of areas. Further work is required to address the awareness issue (see Part 1, Q8-Q9, and Part 2, clause 2.2.4).

Additional work is needed to address these issues and challenges. This work needs to formulate and develop new measures and policies for dealing with these security issues. This work needs to be carried out via international co-operation and involve the development of standards, criteria, new and

1. The OECD Guidelines for the Security of Information Systems are available on the Web at http://www.oecd.org/dsti/sti/it/secur/index.htm

revised legislative measures and regulatory controls, as well as emergence of appropriate security technology and management controls to protect information systems, especially in the context of the GII (see Part 2, clauses 2.2.1-2.2.6).

The general conclusion from the responses was that the existing Guidelines are still adequate to address the issues and purpose for which they were formulated. There was also support by many countries that they are in the right format and at the correct level of detail. However, there is a need to take a closer look at the more recent security issues and legal challenges mentioned above and to consider what work needs to be done to address these issues (see Part 1, Q12-Q15, and Part 2, clause 2.2.6).

The OECD has an important future part to play, in particular the role of a focal point for international co-operation and discussion on future security matters (see Part 2, clause 2.2.5).

PART 1: SUMMARY OF RESPONSES

1.1 Introduction

The purpose of the review (and the associated questionnaire) is to:

- inform and co-ordinate the views of OECD Member countries with regard to the application of the 1992 Security Guidelines;
- survey current practices, implementation, experiences and expectations related to the 1992 Security Guidelines;
- analyse, from a legal and policy perspective, developments since 1992 and the current status of issues concerning security of information and communications systems in the GII/GIS;
- study new information security issues which a review of the 1992 Security Guidelines might need to address;
- collect information concerning future work on security of information systems in the OECD.

This part of this report provides a summary of the responses to the questionnaire that was sent out to all OECD Member and ICCP observer countries as a part of the planned review of the 1992 Guidelines for the Security of Information Systems. This summary highlights the main comments and overall consensus of opinion with regard to the 15 questions that were asked.

The Annex to this report provides a summarised version of each of the responses in tabular form. It should be noted that there were three separate responses from Japan.

At the time of preparation of this report responses had been received from Australia, Austria, Finland, France, Germany, Ireland, Italy, Japan, Korea, Norway, Portugal, Sweden, Switzerland, the United Kingdom and the United States. In addition a response was received from Interpol/Helsinki.

1.2 Overall Summary

I Implementation

Q1 Have the 1992 Security Guidelines been implemented in your country by the public and/or private sector?

Since the adoption of the OECD 1992 Guidelines most of the Member countries have implemented and widely promoted the Guidelines in one way or another. This includes cases where existing measures (guidelines or legislation) are considered to be consistent with the OECD Guidelines. In other cases initiatives to enact new or to modify existing measures have been undertaken. In addition, there are some cases where the Guidelines have been used or referenced as background material in reports, recommendations and in conferences.

Q2 What measures, practices, procedures, laws, policies or agreements have been enacted in your country, by the public and/or private sector, to implement the 1992 Security Guidelines?

Member countries have used various types of measures to implement the OECD Guidelines. These include:

- creating new legislation or revising and amending existing legislation, developing and enacting regulations;
- developing action plans for the implementation of security;
- developing standards, technical criteria, codes of practice, manuals;
- developing methodologies and supporting complementary guidelines;
- creation of agencies, commissioning and advisory bodies, and police units;
- co-operation between supra- and international partners.

In addition, where no direct or immediate implementation has taken place the following measures have also been used:

- development of recommendations on information systems security, including principles and practices, using or referencing the OECD Guidelines as background material;
- distribution and publishing of the Guidelines.

Q3 What projects have you undertaken or participated in, related to security issues in the development and use or management of information systems?

Member countries have been involved in various types of projects covering a broad set of topics and activities including:

- development of standards, guidelines, manuals, handbooks, policies and recommendations at the national, regional and international levels;
- studies and research projects at the national and regional levels;
- organisation of conferences, seminars and workshops;
- international projects and activities e.g. within OECD, international police co-operation;
- EU and Council of Europe projects and studies;
- evaluation activities (e.g. creation of evaluation centres, evaluation schemes, mutual recognition, Common Criteria, protection profiles);
- establishment of a Council or Commission for IT security to co-ordinate policy and measures;
- translation and publication of international level guidelines and green books for security issues.

II Evaluation of Government Policies

Q4 What problems or defects have you encountered in developing measures, practices, procedures, laws, policies or agreements, at the national and international level, related to security issues in the development, use or management of information systems?

Member countries reported the following problems or defects:

- legal constraints on international co-operation and the differences in the various legal systems and how they deal with security matters e.g. such as legal acceptance of digital signatures between different countries, or regulation on computer viruses and on computer crimes;
- lack of resources to implement policy;
- growth in the number of security risks due to increased connectivity of information systems;
- lack of public awareness regarding the vulnerabilities of information systems;
- transborder data flow;
- lack of top management involvement in security issues, communications problems with administrators and decision makers, and lack of awareness;
- in some countries there is a lack of ministries or agencies, and supporting legislation or policy to deal with security matters;
- growth in technological development not being accompanied by effective security measures and policy, also an immature market for security products and solutions;
- management of public-key certification and encryption for international EDI and electronic commerce;
- need for further studies and developments in the field of security evaluation;
- general need to harmonise data protection laws;
- need for a risk assessment based approach to information security.

These problems reflect a continuing need to address legal and policy issues that still restrict and constrain the use and management of security solutions and measures at the national and international levels. There is also a need to address a number of management issues, as well as problems related to changes in technology and the way it is used e.g. increased connectivity and use of the Internet and emerging GII applications.

Q5 What further issues related to the security of information systems have emerged since the adoption of the 1992 Security Guidelines?

Member countries identified the following further security issues:

- security issues related to the Internet, GII and networking in general;
- wireless telecommunications;
- review of access control models, usage and management:
- security of electronic cash, electronic documents and commercial transactions;
- electronic identification;
- secure data interchange for international trade;
- consequences and impact of international standardisation for information systems security;
- measures to deal with problems related to natural disasters;
- computer viruses;
- legal recognition of digital signatures;
- data protection issues;
- protection of intellectual property;
- risk assessment based information security;
- implementation of techniques for digital signatures and encryption, and information security of third parties.

Again a number of these issues are related to networking, the Internet, the GII and use of associated applications and technology. There are also a number of legal issues that need to be considered that are related to the use of these networks and information systems e.g. for international trade, as well as managerial, technical and administrative instruments.

III Consideration for Future Policies

Q6 What policy measures might be taken in the future in your country for the security of information systems?

The following measures were identified by one or more countries, in some cases the measures are purely national in nature while others are more international in nature:

- evaluation and certification of software and hardware in safety critical applications;
- implementation of the OECD Cryptography Policy Guidelines;
- systematic promotion of evaluated and certified products; development of certification schemes;
- introduction of appropriate legislation and regulations for the security of information systems;
- providing a legal foundation for some aspects of electronic commerce and security;
- legislation on digital signatures and electronic documents;
- establishment of public-key infrastructure, certification authorities and Trusted Third Parties (TTPs) including licensing arrangement for TTPs;
- accredited certification against BS7799;
- promotion of research and development activities to improve security of information systems;
- harmonisation of methods for expressing security needs, assessing security levels and identifying security objectives in both the public and private sectors;
- implementation of appropriate internationally standardised security technologies;
- continuation and improvement of information flow to the general public and private sector.

Developments in information security and related policy measures continue to be examined and dealt with at a number of different levels and in a number of important areas. For example, continuation of policy development in some of the emerging areas related to the use and application of the GII is of major importance, e.g. related to electronic documents, digital signatures and Trusted Third Parties. Also policy measures related to security evaluation, standards and future harmonisation of security methods for assessing security needs is of importance.

Q7 What are the most important challenges facing the legal system concerning security issues in the development, use or management of information systems?

The following challenges were identified by one or more countries:

- privacy legislation in the new technological environment;
- laws and practices regarding the creation and maintenance of transnational records concerning information systems to support security and privacy;
- lack of expert resources in the legal system to deal with security issues;
- finding ways and means to settle and resolve national and transnational conflicts and trade disputes;
- legal support for commercial use, and international co-operation, with regard to security and the Internet, the GII, electronic cash, electronic identification and electronic documents;
- evidential value of electronic documents and IPR/copyright issues of Internet documents;
- national and international legislation and supporting counter measures to guard against unlawful and unauthorised access to information systems and computer viruses, especially in the context of networks such as the Internet;
- trusted systems and processes for dealing with electronic documents;
- finding a means whereby the regulations governing data protection can be measured;
- legal basis for the use of 'sensitive' information systems;
- developing identification mechanisms;
- determining jurisdiction over activities on networks.

There is a great deal of overlap between these challenges and the future security issues related to Question 5. A number of these challenges relate to networking, the Internet, the GII and associated applications e.g. electronic documents. Addressing the legal aspects regarding the commercial use of the Internet and the GII is of immediate importance.

IV Awareness

Q8 How would you describe the level of awareness of the importance of security issues in the development, use or management of information systems by government and other public sector institutions, the private (enterprise) sector and individuals?

There was a range of opinions regarding the level of awareness from low to above average. Generally awareness seems to be growing in most countries, promoted by a number of national activities and the use of new technologies. In addition, recent national and international security incidents and natural disasters (e.g. the Japanese earthquake) have raised the level of awareness. One Member country could not provide an answer on the grounds that a specific survey of public and private sector organisations had not been carried out.

There is a need for increasing awareness across all security areas, however, there is also a more concentrated effort needed on some specific topics and issues. For example, the awareness related to administrative, management and personnel matters is somewhat less developed than the awareness of the security issues related to the use of technologies.

The awareness amongst major companies and organisations is greater than that of SMEs (Small and Medium sized Enterprises).

Q9 What measures have been used to improve awareness of the 1992 Security Guidelines or security of information systems in general?

The Guidelines have been made available to a large audience of readers and they have been referenced in many reports, documents, press releases and recommendations, at both the national and international level. They are generally seen as being instrumental in promoting awareness and have been used in training materials and courses.

The following measures were identified as having been used to improve awareness:

- increase in the number of training and educational courses for information systems security for both the public and private sector, this includes the means of being able to obtain professional and academic qualifications;
- establishment of computer emergency response teams and associated co-ordination centres for handling security incidents and disseminating information on such incidents and solutions to resolve related security problems;
- amendment and revision of existing manuals, codes of practices and other guidelines to take into account new security issues;
- promotion of security issues through seminars, workshops, conferences, standards groups;
- publications and dissemination of translations of the Guidelines;
- introduction of new laws, regulations and guidelines based on the Guidelines.

V International Co-operation

Q10 Has your country been involved in any efforts to improve international co-operation on information security issues?

The following activities were reported as being instrumental in improving international co-operation:

- OECD Expert Groups;
- international standards bodies e.g. ISO/IEC JTC1/SC27, IEEE;
- other standards bodies e.g. CEN in Europe;
- Council of Europe, EU and EC activities including those of SOG-IS;
- Police Co-operation Working Group;
- evaluation criteria work e.g. the European ITSEC work and the work of the Common Criteria Editorial and Implementation Boards;
- close contact with international partners, governments and industry on security issues and collaborative projects and studies;
- international conferences e.g. OECD conference on 'Security, Privacy, Intellectual Property Protection in the GII' and the international conference of the Data Protection Commissioners, workshops and seminars.

Q11 What measures might be taken to improve international co-operation on issues relating to the security of information systems? Is there a future role for the OECD?

Various ideas have been put forward to improve international co-operation. An overriding opinion that has emerged is that the OECD is ideally placed to continue to act as a forum for discussion, debate, the exchange of information and the improvement of international co-operation.

The following are some specific suggestions for improving co-operation on security issues:

- the OECD should act as a forum for international co-operation on security issues;
- the OECD should set up a permanent observatory on information security;
- the OECD should co-ordinate its work with that of the EU;
- the OECD could be used to test the relevance of security principles before they are made directly applicable or deemed binding within another framework;
- work on specific security problems such as GII and Internet security, the security of transactions in a transnational context, international recognition of digital signatures, public key infrastructure functions, the ongoing work of OECD on crypto guidelines and those other issues mentioned in Q4 to Q7.

VI Revision of the Guidelines

Q12 In view of developments over the past five years, are the 1992 Guidelines still adequate? Should they be amended, extended, or otherwise modified? Should a new start be made on an entirely revised set of Guidelines?

The general opinion is that the Guidelines are still adequate and no major revision of the existing text needs to be undertaken. There were some comments which indicated possible areas of extension and the need to review the application of the Guidelines principles in the context of the new environment in which information systems are used. Since the Guidelines were published in 1992 the scope of security has widened e.g. due to the increased connectivity between information systems and the use of the Internet. A country suggested that the OECD should consider extending the Explanatory Memorandum to adapt to these new circumstances. Areas of possible future extension of the Guidelines are:

- security of wireless communications, networks, services and interconnecting information systems; for example (i) firewalls, (ii) e-mail and file transfer, (iii) on-line telephony, (iv) TTPs and (v) electronic cash;
- improvement to the telecommunications infrastructure;
- electronic identification systems.

In addition to the above, there was another view from one country that the Guidelines are at such a high level of abstraction as to be of marginal use in implementing day-to-day security solutions, however they do provide a possible framework for such implementations. Another country suggested that the Guidelines language could be simplified and its clarity be improved.

Q13 Should the Security Guidelines also cover information security in addition to security of information systems?

There was a general opinion that the term 'information security' should be clearly defined. Others disapproved of the proposal to change the scope of the Guidelines to cover 'information security'.

On the other hand, a few responses were in favour of covering the concept of 'information security', especially if it leads to a broader scope e.g. if it covers information in networks, computer viruses and aspects of data protection and privacy.

Q14 Would the 1992 Guidelines be more useful in a different format or at a more detailed level?

The responses were of two types: those that found the format and level of detail sufficient (the majority of responses) and those that would appreciate more detail, or greater clarity. One opinion stressed the importance of not changing the current set of Guidelines since that could influence and impact initiatives that have been undertaken to implement the Guidelines. Another opinion stated that more detailed sets of guidelines already existed at the national level and so the level of detail of the OECD Guidelines is adequate. This was supported by another response which stated that due to differences in priorities and requirements a sufficiently detailed set of guidelines, both relevant and suitable for implementation at the national level, cannot be written at the international level.

Q15 Is there a need for a set of Guidelines with a wider scope than the 1992 Guidelines which might encompass or even replace them?

The general opinion was that there was no need for a set of guidelines with a wider scope. However, other responses suggested, in line with answers to questions 12, 13 and 14, that there was a need to either have a set of guidelines with a greater level of detail or that various new areas should be considered to extend the current Guidelines. One view was that the convergence of technologies has resulted in an overlap of issues relating to security, privacy, IPR, consumer issues, government revenue generation, law enforcement and electronic commerce. Therefore rather than replacing the existing Guidelines they should be reviewed to provide an overarching set of principles that would encompass the existing set and would ensure a consistent approach to the different issues.

PART 2: RECENT ISSUES, CONCLUSIONS AND FUTURE ACTION

2.1 Recent Developments and Issues

Over the past five years there have been some significant changes with regard to the development and use of information and communications systems. Certainly the Internet has played a major part in shaping the way companies and organisations do business and how the individual citizen communicates and exchanges information. On-line services, electronic commerce, electronic cash, multimedia information are all-too-familiar terms to a growing world community of citizens. Mobile and wireless networks are being integrated together with the Internet and Intranet developments to provide a seamless communications network for both the business and the private citizen. The emerging GII/GIS scenario takes us along this path towards the next generation of information systems. All these developments are presenting new security issues and new risks that need to be dealt with from a technical, legal and policy perspective. The further security issues that have emerged since adoption of the Guidelines include:

- security issues related to the Internet, Intranet, GII and networking in general;
  - securing on-line services and applications, electronic cash, electronic documents and commercial transactions, secure data interchange for international trade;
  - electronic identification;
  - mobile and wireless telecommunications;
  - need for improved access control models, and policies;
  - computer viruses and other malicious pieces of software;
- measures to deal with problems related to natural disasters;
- legal aspects, for example;
  - constraints on international co-operation;
  - acceptance and recognition of digital signatures between different countries;
  - transborder data flow;
  - lack of expert resources in the legal system to deal with security issues;
  - finding ways and means to settle and resolve national and transnational conflicts and trade disputes;
  - legal support for commercial use, and international co-operation, for the GII;
- implementation of techniques for digital signatures and encryption, and security of public-key infrastructure and Trusted Third Parties.

Some of these issues are not necessarily that new, however, they have become more significant since the threats and risks and their potential impact on an organisation's information system and connectivity to outside networks has greatly increased and diversified.

Related to these issues are aspects of privacy and data protection, intellectual property protection and cryptography policy. In addition, there are aspects related to the use, management, standardisation and evaluation of information systems e.g. in a GII environment, which need to be considered in the context of the above issues.

These issues should also been seen in the light of other developments, for example standards developments and collaborative research programmes.

Within the international standards community there are also various relevant activities appropriate to the security of information systems. For example within ISO/IEC JTC1/SC27 there is work in progress on Guidelines for the Management of IT Security (GMITS) which considers the risk assessment, code of practice and baseline control approaches to security. In addition, SC27 is responsible for the international standardisation of security evaluation criteria. This work is being developed in collaboration with the Common Criteria Implementation Board. SC27 also develops standards for security techniques e.g. for integrity and authentication.

Other relevant security standardisation work is also progressing in other ISO/IEC Committees, in various European groups such as security of healthcare informatics in CEN (Comité Européen de Normalisation), Trusted Third Parties in ETSI (European Telecommunications Standards Institute) and OSI security in EWOS (European Workshop for Open Systems), and at various national levels (e.g. the United States, Canada, Australia, New Zealand, Japan and the European countries). There is also work going on at the Internet level through the work of the Internet Engineering Task Force (IETF), in IEEE and the Open Group (X/Open and OSF).

Within the EU various other security activities have taken place such as the European Commission's INFOSEC programme and the work of SOG-IS (Senior Officials Group on Security), and various collaborative research programmes e.g. ACTS (dealing with advanced communications), Telematics (dealing with topics such as healthcare and administrative networks) and TEDIS (dealing with EDI issues). Also there have been activities within the Council of Europe on computer crime and law enforcement. The EPHOS (European Procurement Handbook for Open Systems) also now includes security as a topic. There are many other important security initiatives and projects that have developed over recent years across Europe in the various Member States and in other countries in the world.

2.2 Conclusions and Future Actions

2.2.1 Implementation

In general, the OECD Security Guidelines have been implemented, supported and promoted in most Member countries. This has resulted in the enactment of legislation, development of standards, technical criteria and other regulations. It has also lead to the initiation and participation in a number of projects at national, regional and international levels (see summary of responses to Q3 for list). Also the private sector has used and referenced the Guidelines as a basis for its management and technical procedures.

Suggested Action

. Continued promotion of the Guidelines, and development and adoption of new measures to implement the Guidelines by Member countries is appropriate.

2.2.2 Evaluation of Government Policies

In evaluating government policies various problems have been encountered related to security issues in the development, use or management of information systems. Some of these relate to legal aspects (e.g. legal constraints on international co-operation), some are technical aspects (technical security risks due to increased connectivity of information systems) and some are management aspects (e.g. management of public-key certification and encryption for international EDI and electronic commerce). A list of these issues is given in the summary of responses to Q4.

In addition, a number of future issues have been identified, again these cover legal, technical and management aspects of security. A list of these issues is given in the summary of responses to Q5.

Suggested Actions

· The list of problems and future issues (Q4 and Q5) should be considered by the OECD Group of Experts as a suitable topic list for reviewing the Guidelines and for discussion topics at a future conference should it organise one.

· Further suggestions made in response to Q4 and Q5 may be found in part II of the Annex.

2.2.3 Consideration for Future Policies

A range of policy measures have been identified for future action by the Member countries. Some of these relate to national issues and other relate to international issues. A number of these measures are associated with the security evaluation of products and applications, some relate to the legal aspects of security, implementation of the OECD Cryptography Policy and others include public-key infrastructure and trusted third parties. A full list of these future policy issues is provided in responses to Q6. One can conclude from this that there are a number of significant activities being planned to support and implement security for information systems.

However, in addition, a number of future legal challenges have been identified which need to be addressed. Some of these are national issues and others are concerned with international issues.

Suggested Actions

- The list of future legal challenges (Q7) should be considered by the OECD Group of Experts to decide where these issues can best be dealt with at a national or international level: in some cases there may be a need for action to achieve international co-ordination, and in other cases further discussion may be required to clarify the problem and what is to be done -- some of these issues are strongly related to those identified in the responses to Q4 and Q5.

- To assist in the resolution of the security issues and legal challenges referred to above, and to achieve international harmonisation, Member countries that are directly involved or are working on the same or similar issues should make contributions to the Group of Experts on their findings and results.

2.2.4 Awareness

Everyone recognises the importance awareness plays in understanding and implementing solutions to resolve security issues. Even though the general level of awareness has increased over the last five years there is a continuing need to support awareness activities.

Awareness and training are needed at a high systems level, and at more detailed technical levels. They are also required to deal with administrative, management and personnel matters relating to security. Awareness initiatives and training programmes need to be regularly reviewed and updated to take account of changes in technology and how this technology is used to support an organisation's applications, and the business processes and services it uses.

Suggested Actions

- National awareness schemes and codes of practice should be developed to support public and private sector awareness initiatives and this could be supported by the development of an OECD set of awareness materials and guidelines.

- A review needs to be undertaken at the national level to check how adequate existing security training and educational courses are for both the public and private sector.

- More needs to be done to support and increase the awareness for SMEs.

- Greater use of computer emergency response centres for handling and disseminating information about security incidents should be encouraged.

2.2.5 International Co-operation

Various activities have taken place to ensure greater international co-operation and this effort has been supported by all countries. It is also clear that the OECD has a key role to play in supporting future international co-operation.

Suggested Action

- The OECD should continue to act as a forum for international co-operation and discussion in the field of information security, this includes the suggestions cited in the summary to Q11, and, in addition, the establishment of a permanent OECD Observatory for Information Security should be considered.

- The OECD should look into security aspects of electronic commerce.

2.2.6 Revision of Guidelines

The general conclusion is that the Guidelines still appear to be adequate and the consensus of opinion is that the format and level of detail is sufficient. However, a number of recognised changes have taken place in the field of information systems and networking to warrant consideration of other security issues such as those related to the GII and the Internet, electronic commerce and electronic cash, to name but a few.

Suggested Action

- Based on the responses to the questionnaire, the OECD Group of Experts needs to consider the following:

  - whether the current content of the Guidelines should remain unchanged but some form of extension document needs to be produced to cover those security issues given in responses to Q4 to Q7 and consolidated in Q12;

  - the development of a work programme to take such work forward, particularly on issues concerning electronic commerce;

  - a definition and discussion of the concept of 'information security' should take place to resolve the question of whether the scope of the Guidelines should cover this aspect.

- Those Member countries that require a set of Guidelines with a greater level of detail should first decide what their requirements are and then consider whether this should be done at the national level in order to provide sufficient detail suitable for implementation at that level.

ANNEX: INDIVIDUAL SUMMARIES

The tables that follow provide a summary of each of the individual responses that were received. These tables are a summary only, full details of each of the responses are contained in the Member country contributions received. Every attempt has been made in these summaries to reflect as closely as possible the views expressed in the more detailed contributions.

The following abbreviations have been used in this report:

ANS	Portuguese National Security Agency
BCRCI	Brigade Centrale de Recherche contre le Crime Informatique
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEN	Comité Européen de Normalisation
EC	European Commission
EDI	Electronic Data Interchange
EFT	Electronic Funds Transfer
EICAR	European Institute for Computer Anti-Virus Research
EPHOS	European Procurement Handbook for Open Systems
EU	European Union
EWOS	European Workshop for Open Systems
FISC	The Centre for Financial Industry Information Systems
GII	Global Information Infrastructure
GIS	Global Information Society
II	Portuguese Institute of Information Technology
IEC	International Electrical Committee
IPR	Intellectual Property Rights
ISO	International Organisation for Standardisation
IT	Information Technology
ITSEC	IT Security Evaluation Criteria

JPCERT/CC	Japan Computer Emergency Response Team/Co-ordination Centre
MITI	Ministry of International Trade and Industry
NIST	U.S. National Institute of Standards and Technology
OMB	U.S. Office of Management and Budget
SC	Sub-Committee
SCSSI	Service Central de la Sécurité des Systèmes d'Information
SEFTI	Service d'Enquête sur les Fraudes en Technologies de l'Information
SOG-IS	Senior Officials Group on Information Security
TC	Technical Committee
TTP	Trusted Third Party

I. IMPLEMENTATION

	Q1. Have the guidelines been implemented in your country?	Q2. What measures, practices, procedures, laws, policies or agreements have been enacted?	Q3. What projects have been undertaken or participated in?
AUSTRALIA	High level policy for information technology security in the Commonwealth Government sector is contained in the Protective Security Manual which is consistent with the OECD Security Guidelines.	Standards are under development (in collaboration with New Zealand) for the security of information systems which reflect the OECD Guidelines. Also Commonwealth Government committees are addressing the issues of security as part of the decision making process to ensure an integrated government approach.	Work has been undertaken on the development of a joint Australian and New Zealand standard on information security management based on the UK standard BS7799. This is due to be published soon. A network has been established to address aspects of information security across the public sector, particularly in the area of government electronic services delivery.
AUSTRIA	The Austrian Data Protection Act (nr. 565/1978) includes several provisions related to data security. This covers: (i) confidentiality, (ii) the accountability principle, (iii) the awareness principle and (v) the ethics principle. Also the Penal Code includes legal measures to protect data.	The Federal Government has formed KIT (*Kommission für Informationstechnologie*) and BIT (*Beratungsausschuß für Informationstechnologie*) to co-ordinate the Federation's IT policy which includes data security, procurement and data protection.	The Ministry of Health and Consumer Protection has formed a commission (called STRING) to deal with all aspects of data processing in healthcare. STRING deals with the use of chipcards in healthcare and digital patient records. STRING is in contact with the CEN group TC251 which deals with medical informatics.
FINLAND	Being broad and general they are not implementable. However the Guidelines have been given wide publicity and have provided background and guidance for action both in the public and private sectors. These activities were reported to the OECD in November 1993.	The recommendation on information systems security in government data processing (1993) used the Guidelines as background material.	International projects at the Nordic, EU, Council of Europe, ISO and OECD levels and in international police co-operation.

FRANCE	To a large extent France had already anticipated the OECD Security Guidelines. An explicit reference to these Guidelines appears in the government document 'Politique de Sécurité Informatique' as a contribution to policy making in this area.	Several actions have taken place that are consistent with the Guidelines including: (i) two new units of the national police force were created to investigate and prosecute IT related crimes and misdemeanours: SEFTI and BCRCI, (ii) formulation and utilisation of a methodology to make information systems secure and identify needs up to approval and licensing stage of evaluated products and systems and (iii) the revised criminal code incorporates the Act on Prosecution of Computer Fraud.	Activities include: (i) dissemination of a recommendation (901/DISSI/SCSSI) for the protection of systems that process sensitive information not classified as defence related, (ii) creation of the French evaluation and certification scheme by an Opinion of the Prime Minister and issuance of the first ITSEC certificates in 1996, (iii) progress towards mutual recognition of security certificates for information and communications technology products, (iv) contributions to the standardisation of Common Criteria and (v) proposed protection profiles for network connections having different levels of protection.

	Q1. Have the guidelines been implemented in your country?	Q2. What measures, practices, procedures, laws, policies or agreements have been enacted?	Q3. What projects have been undertaken or participated in?
GERMANY	Most of the important aims of the OECD Guidelines have been implemented in the context of the foundation, by Federal Law, of the German Information Agency (BSI): the tasks of BSI are based on the scope and aims of the Guidelines. In addition, close co-operation between the public and private sector on security issues is taking place.	In accordance with the German Federal Law the government has developed and published two manuals on 'IT Security' and 'IT Baseline Protection'. In addition international co-operation has taken place with its partners to facilitate the use and development of secure information systems. Also, legislation has been developed in the field of digital signatures.	Organisation of conferences on IT security issues to promote the constant and extensive flow of information between the public and private sectors.
IRELAND	The public sector has not implemented the OECD Guidelines. However, it has issued and implemented its own national guidelines in the period 1991-1994. *Note: Ireland has remarked that it did not receive a copy of the Guidelines until 1994*. The response could not comment on behalf of the private sector implementation of the OECD Guidelines.	The national guidelines address specific security needs of the Irish civil service. Implementation of specific measures by Ministries was based on the recommendations of the Office of the Comptroller and Auditor General.	Provision of security advice to Government Ministries, participation in various fora, educational/awareness initiatives at the national level, and in the EPHOS project at the European level.
ITALY	The Guidelines have not been implemented by any sector in Italy.	See answer to Q1.	The security issues in the public sector have been examined by the Autorita per l'Informatica nella Pubblica Amministrazione (AIPA) in the context of the 1995-97 Public Administration's information plan established in June 1994. In January 1996, AIPA prepared a feasibility study concerning the Administration's unitary information network, which includes security issues.
JAPAN	The OECD Security Guidelines have been implemented in Japan. They are referenced in the MITI announcements 'The Information Systems Security Guidelines' and 'The System Auditing Guidelines'. The private sector has voluntarily adopted and implemented the guidelines. FISC (The Centre for Financial Industry Information Systems) published its Computer System Security Guidelines in 1985 (revised in 1991).	The MITI announcements mentioned in Q1 were amended in 1993 and 1994 respectively to include aspects of the OECD Guidelines which had not been included in the earlier versions. The 'Security and Reliability Standards of Information Networks' was developed in 1987. These standards are in line with the OECD Guidelines. FISC is developing Security Guidelines for financial institutions.	The Security Evaluation Criteria Development Project. A special study group meets annually to improve security and reliability of networks. The purchase and use of equipment for the reliability and security of information systems is linked with tax reductions. FISC produced a handbook 'Contingency Planning for Financial Institutions'. FISC has undertaken a study into how to maintain a financial network in case of earthquakes and it has researched into the question of back-up centres.

	Q1. Have the guidelines been implemented in your country?	Q2. What measures, practices, procedures, laws, policies or agreements have been enacted?	Q3. What projects have been undertaken or participated in?
KOREA	The OECD Security Guidelines have been implemented in Korea by the public and private sectors.	The technical criteria for the security and safety of computer networks have been enacted by "Law of Growing interconnection of network and promotion of use". The law also covers computer network security management guidelines as well as protection of information and privacy by the public and private sectors.	A project is being undertaken to develop a policy for safety, reliability and information security of information systems by implementing OECD cryptography policy guidelines.
NORWAY	The Security Guidelines have been implemented in different ways: (i) they have been translated into Norwegian and given a wide distribution in public and private sectors (this includes a preface recommending the guidelines to be followed), (ii) the Norwegian centre for EDI and trade procedures (Norsk EDIPRO) has developed draft guidelines for Norwegian TTPs based on the principles in the Guidelines, (iii) the intent of the Guidelines is to a certain extent covered by the Norwegian Data Security Directive of 1989, published by the Defence and valid also for governmental administration handling classified information (this Directive is now being revised, and especially the proportionality Principle will be taken account of), (iv) the Norwegian Industrial Security Council has published the booklet "How to protect Your Business against Datacrime" and "Security of Information Systems and Ethics" will follow next year, and (v) the Norwegian Centre for Medical Informatics has published a booklet "High level information security policy for the health care sector" based on, among others, the OECD Guidelines. This booklet will be revised in 1997 with the objective of making it a health care standard sanctioned by the Ministry of Health and Social Affairs.	Recommended best practices for information security has been developed for the public sector. A revised version, which broadens the scope and integrates information systems security with other security considerations, is now at a final stage. The Norwegian Data Inspectorate has developed and enacted regulations for the secure handling and distribution of personal information including requirements for the development of security policies. The Ministry of Health and Social Affairs has developed a four year action plan for the development of IT in health care, where privacy and information security are major components. In the implementation of this plan the OECD Security Guidelines will be used as an important basis.	Projects include: (i) a Council for IT-security has been established in order to co-ordinate policies and measures on IT-security, (ii) a certification scheme for IT security products is under consideration, (iii) ITSEC has been adopted in Norway as the recommended criteria, (iv) Norsk EDIPRO are making implementation guidelines for the use of digital signature schemes in EDI messages, and (v) secure messaging infrastructure for the health care services, involving EDI, email, telemedicine and TTP services has been initiated. This infrastructure will offer secure interoperability with similar infrastructures in other sectors.

	Q1. Have the guidelines been implemented in your country?	Q2. What measures, practices, procedures, laws, policies or agreements have been enacted?	Q3. What projects have been undertaken or participated in?
PORTUGAL	The Institute of Information Technology (II) translated the Guidelines and published them in a special issue of its review *Informaçao é Informatica* which, at the time of publication, had a circulation of 200 and was distributed to many sectors of activity. The principles underlying the Guidelines have been widely published and have had a major impact on various sectors of activity.	Order in Council No. 47/93 recasting the Organic Law of the Ministry of Defence. Article 15 of this new Act provides for the creation of a National security Agency (ANS) whose jurisdiction includes *inter alia* the security of secret information, personal/physical security and security of communications and information systems. Law No. 65/93 regulates access to documents produced or held by government bodies or agencies. Implementing Decree No. 27/93 setting out rules to ensure that central public services comply with the Guidelines with respect to personal data. Law No. 28/94 authorising measures to enhance the protection of personal data. Resolution of the Council of Ministers, No. 16/94 (Security of Guidelines). Order of Council, No. 252/94 translating EC Directive No. 91/259/EEC (Legal Protection of Software) into domestic law.	The ANS, II and the IPC (Portuguese Institute of Communications) have promoted the publication of Portuguese versions of the following texts: The Green Book on the Security of Information Systems (European Commission DG XIII). ITSEM (Information Technology Security Evaluation Manual) (European Commission DG XIII).
SWEDEN	There have been no Government decisions regarding its implementation. However, the Guidelines have been made available to a large number of organisations and people in 1992/93. They were also referred to in the final report to the Ministry of Finance (report produced by the Government Co-ordination Committee on IT Security).	See answer to Q1.	There have been a large number of projects in Sweden since 1992 both in industry and government. A complete list of these activities is presently not available. Some of the major activities include: (i) Swedish participation in EU work on IT security, (ii) specification of requirements for the secure workstation, (iii) establishment of the association 'Secure Electronic Information in Society', (iv) security work related to IT in Government through the 'Top Managers' Forum (headed by the Minister of Finance) and (v) participation in the OECD work on Cryptography Policy Guidelines.

	Q1. Have the guidelines been implemented in your country?	Q2. What measures, practices, procedures, laws, policies or agreements have been enacted?	Q3. What projects have been undertaken or participated in?
SWITZERLAND	Some of the OECD Security Guidelines have been implemented both in the public and private sectors.	Data Protection Law (public and private) and Data Security Policies for the public sector.	Projects include the planning and implementation of sensitive information systems and security measures by the Federal Government. This is overseen by the Data Protection Commissioner.
UNITED KINGDOM	The principles outlined in the OECD Guidelines are complementary to developments in the field of information security over the past five years. In particular, the development of BS7799 (A Code of Practice for Information Security Management) has promoted a wider adoption of the principles of good practice for information security.	The principles outlined in the Guidelines are consistent with the development of the UK standard BS7799. This standard has been widely reviewed, both in the UK and in other countries, and has received widespread recognition and support. Adoption of this standard is on a voluntary basis.	In addition to the development of BS7799, there is a scheme being developed for accredited certification against this standard. Other UK projects have resulted in the publication of various documents including : (i) 'Business Manager's Guide for Information Security', (ii) 'Protecting Business Information - Understanding the Risks' and (iii) 'Protecting Business Information - Keeping it confidential'.

	Q1. Have the guidelines been implemented in your country?	Q2. What measures, practices, procedures, laws, policies or agreements have been enacted?	Q3. What projects have been undertaken or participated in?
UNITED STATES	The Guidelines have been extremely well received in the US. Several initiatives have been undertaken, but full implementation and use is still somewhat constrained by the lack of public awareness of the Guidelines at the worker level.	NIST has issued three documents: 1) *An Introduction to Computer Security: the NIST Handbook* (Special Publication 800-12, Oct. 1995) introduces an NIST-developed approach to computer security, which consists of eight elements based on the Guidelines. 2) The re-publication of the elements presented in NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Security Information Technology Systems*. 3) A CSL Bulletin (a more informal publication) on generally accepted principles and practices. In February 1996, OMB issued an update to OMB circular A-130, Appendix III, Security of Federal Automated Systems to provide a policy framework and specific minimum security activities for federal systems. In 1996, the primary US federal law dealing with computer crime, 18 USC §1030 (the Computer Fraud and Abuse Act) was amended to better protect the confidentiality, integrity and availability of data and systems.	The US Federal Government has participated in numerous activities relative to security issues. The US private sector, through individual corporations, standards and trade organisations, as well as academia, participated in numerous domestic and international efforts. Particularly noteworthy are recent decisions by the President to create a Commission on Critical Infrastructure Protection and an Information Protection Task Force. Within the private sector, several efforts are underway to establish generally accepted security principles and practices. All of the work on principles of development is based on the Guidelines. But, to date, no working documents have been produced.
INTERPOL (HELSINKI)	The Guidelines have been implemented and will continue to be used in the context of the Protective Policing efforts. The 'Information Security Policy Decisions' have been widely distributed and they include the whole of the OECD Guidelines.	Legislation such as the amendment to the Coercive Powers Act and the International Legal Assistance in Criminal Matters Act enforces the Timeliness Principle. Other pieces of legislation are also supportive of the Guidelines.	Council of Europe Recommendation concerning problems related to criminal procedural law connected with IT. Interpol Conference 'Computer Crime and Electronic Evidence' - 1996. An EICAR Conference paper on 'Legal Infrastructures and Malicious Code'.

II. EVALUATION OF GOVERNMENT POLICIES

	Q4. What problems or defects have been encountered?	Q5 What further security issues have emerged?
AUSTRALIA	The Australian Government approach has been not to regulate information security with the exception of the protection of personal information. Instead a self-regulatory approach is used based on national standards which allow for greater flexibility for responding to changes in technology. To date no problems have been encountered with this approach, although the EC Directive 95/46/EC has yet to be assessed.	The expansion of the Internet has resulted in a fundamental change in the paradigm for information security. The emergence of the independent user who can access numerous information systems has resulted in fundamental changes in access control philosophies. It is now time to review and examine the relationships between the user and methods for access control, and how these methods are being used in practice. Techniques for anonymous access and the dependence on the information transmitted via the GII need to be reviewed.
AUSTRIA	(i) Control of data security measures requires resources (money and people) which are difficult to acquire during the government's austerity programme. (ii) Increase in the number of security risks due to the increased connectivity of information systems and the use of LANs, MANs, WANs and the Internet. (iii) Transborder data flow.	Use of networks and wireless telecoms technology for data transfers has increased (e.g. eavesdropping, transmission performance, loss of integrity).
FINLAND	The following are seen to be problems: (i) lack of top management involvement in security issues; (ii) lack of legislation on, and a ministry or agency with a clear mandate to act on security matters; (iii) lack of progress in the EU on these matters; (iv) lack of legislation of administrative mandate.	Commercial use of the Internet, electronic cash, and electronic identification.
FRANCE	The usual security problems encountered at the national level (e.g. lack of reporting of IT security incidents). Also legal constraints on international co-operation.	A lack of concerted effort on the part of competent authorities to anticipate the consequences of international standardisation in the field of information systems security (e.g. common criteria, communications protocols and security management for the Internet and for medical records). The emerging GII and the existing Internet are not sufficiently secured or managed properly. There is a clear need for proposals that take cognisance of the risks involved, and that define how techniques and their utilisation can be made secure. Access to secure data interchange for international trade.
GERMANY	Growth in technical developments can be a problem if it is not accompanied by effective security measures and policies.	Internet security.
IRELAND	The general tendency to promote the use of single and specific technological solutions to general security problems rather than adopt a risk analysis approach and the implementation of baseline controls.	Commercial transactions over the Internet, authentication and integrity of electronic documents.

	Q4. What problems or defects have been encountered?	Q5 What further security issues have emerged?
ITALY	There is no real government policy as regards the security of information systems. Each public or private organisation implements, in the information systems field, procedures of varying levels of security while awaiting proper co-ordination, at least in the public sector. In the absence of concrete directives for the security of information systems it is impossible to assess the problems and defects in this field.	See answer to Q1.
JAPAN	More study is required with regard to security evaluation criteria. Differences in the legal system of Japan compared with those of the USA and Europe, especially with regard to the lack of legislation on computer viruses and anti-invasion of computers. Studies into methods for dealing with certification and encryption of EDI are taking place.	Measures to deal with natural disasters (e.g. the effects of information systems being shut down due to earthquakes). Also Internet problems related to computer viruses and illegal usage of, and unauthorised access to networks.
KOREA	There is a problem in evaluating the system of information security due to lack of internal evaluation criteria.	The lack of useful tools for the protection of information which is processed, stored and communicated, has emerged as a serious problem since the adoption of the 1992 Security Guidelines.
NORWAY	Problems or defects include: (i) immature market for security products and solutions, (ii) insufficient awareness on security issues, (iii) communications problems with administrators/decision makers, due to perceived complex substance and narrow expert terms in the field of information systems security, (iv) the Media has expressed a general fear that security measures and regulations will hinder the Media access to government information, and (v) insufficient legal framework in the sense that IT and new forms of communication and interaction - also at the organisational level - are not covered by existing (sector) legislation.	In general, the whole spectra of problems related to the contradictions between the need for trust and security of information systems on the one hand, and the wish for open networks, electronic trade and democratic exchange of information on the other. Other issues include: (i) the focus on digital signatures, TTP, crypto, electronic mail, (ii) the relation between closed networks and Internet, and (iii) in government administration, a broad range of questions have been raised that are related to security in case handling and archiving.
PORTUGAL	There is no real government policy concerning the security of information systems. The responsibilities of the ANS are expected to be increased in the near future and changes made to its overall management structure.	The following themes should be discussed in depth with a view to harmonising current differences in approach: 1) protection of personal data and privacy; 2) enhanced security of information systems; 3) policy on cryptography; 4) protection of intellectual property; 5) the managerial, legal, technical and administrative instruments to be used to achieve the above objectives.
SWEDEN	Individual OECD Member countries are not prepared to legally recognise digital signatures from other Member countries.	Legal recognition of digital signatures at the international level.
SWITZERLAND	Harmonisation of the different data protection laws across Switzerland takes time.	Data Protection issues and Data Security Policies for the public sector.

	Q4. What problems or defects have been encountered?	Q5 What further security issues have emerged?
UNITED KINGDOM	It is important to recognise, and promote, the need for a risk assessment based approach to information security, which recognises the value of the information as an asset to the organisation. The 1992 Guidelines confined themselves to information systems but, in our view, it is the information contained in those systems that should be the primary focus for security measures. There is a need for both management and technological solutions.	Issues include: (i) risk assessment based information security rather than security for information systems, (ii) emerging technological issues such as those posed by the Internet, (iii) techniques for digital signatures, encryption and non-repudiation need to be addressed, and (v) information security of third parties.
UNITED STATES	Lack of public awareness regarding the vulnerability of information systems. Many victims of computer crime are reluctant to report it, which hampers law enforcement's efforts to deter crime though investigation and prosecution. Furthermore, there is the difficulty in developing laws and practices that properly address emerging technologies. The widespread use of information systems, for example, at levels ranging from infrastructure level systems to small electronic appliances, makes the development of laws of appropriate scope difficult.	The most significant security issues are those related to encryption and the need for a wider availability of public key infrastructure. Among the most significant legal/investigatory issues are the need for technical means of tracing attacks on information systems and the need to develop, on an international level, mechanisms to investigate such attacks in real time.
INTERPOL (HELSINKI)	The need to include the demand for IT security into the 'Public Procurement Act' and into the 'Companies Act'.	Internet security, cryptography and OECD cryptopolicy.

III. CONSIDERATION FOR FUTURE POLICIES

	Q6. What policy measures might be taken in the future?	Q7. What are the most important challenges facing the legal system concerning security?
AUSTRALIA	Developments in IT and its impact on security will continue to be examined at both the government level and in Standards Australia to develop policy and technical solutions. One specific issue that is currently being addressed is the evaluation and certification of software and hardware in safety critical applications. Standards Australia has already included such a provision in a standard relating to health information systems.	Australia does not take a legislative approach to IT security. However, electronic commerce and user access to government information are emerging as major issues. The legislative approach to electronic commerce is likely to use standards to address security issues. Privacy legislation may need to address the question of security of personal information in the new technological environment but this might use some form of standards approach.
AUSTRIA	Policy measures for the implementation of the OECD Cryptography Guidelines.	The legal system needs more resources to meet the challenge of a legal and social environment which is dependent on the integrity and availability of information systems.
FINLAND	Development of appropriate legislation.	Legislation to support the commercial use of Internet security, electronic cash and electronic identification. Security of commercial and administrative services provided through networks.
FRANCE	Measures include: (i) harmonisation of methods for expressing the needs and identifying security objectives, in both the public and private sector, and (ii) systematic promotion of products evaluated and certified as responding to market expressed needs for protection.	The challenges facing national and transnational legal systems are to find quick and transparent ways to settle conflicts and trade disputes, in particular, without encroaching upon the prerogatives of States or violating individual rights.
GERMANY	Development of policy for the use of cryptosystems taking into account the use for transnational data flows.	Legal basis for international co-operation with regard to the GII.
IRELAND	Continuation of the policy to maintain the security of information and to implement, as appropriate, internationally recognised and standardised security technologies.	The evidential value of electronic documents and IPR/copyright issues on Internet documents.
ITALY	See answer to Q3.	Only a few laws have been enacted concerning the security of information systems in the public sector. There are Directives *from Autorita Nazionale della Sicurezza* (relating to the security of state information processed by computers). There are also other measures introduced by a Decree of the President of the Republic (relating to data processing). Measures on personal data protection are contained in a bill introduced by the Minister of Justice in June 1996, this is at present before the Parliament for examination. There have been modifications to the Penal Code to deal with unlawful access to information in a computer or data transmission system protected by a security measure.

	Q6. What policy measures might be taken in the future?	Q7. What are the most important challenges facing the legal system concerning security?
JAPAN	Measures include: (i) establishment of security evaluation criteria, (ii) continuation of providing information on security measures to private sector, (iii) promotion of research and development to improve security of information systems and (iv) possible assessment of the security level accomplished by private sectors being considered by both the public and private sectors.	With the increased use of networked systems one of the most important challenges is the protection of information systems from unlawful access. MITI has produced a set of guidelines entitled 'Protection for Unlawful Access to Computers' - August 1996. Another challenge is the international harmonisation of counter measures to guard against computer viruses and unauthorised access to information systems.
KOREA	The detailed policy for information security in the public sector will be redefined in the future.	Maintaining a balance between public security and privacy is one of the most important challenges facing the legal system.
NORWAY	Eventually a national scheme for certification of security products. Also a system for administration of public keys for digital signatures and crypto. The Data Inspectorate is in the process of developing new regulations for the communication of health care and other sensitive information, including policies for connecting to Internet. These regulations were to be finished spring 1997. The Ministry of Health and Social Affairs is also in the process of developing new regulations for the use and security of IT and communication technologies in the health care sector.	The greatest challenge for the legal system concerning computer security concerns the definition of which methods of electronic transmission and storage are sufficient in respect of different levels of secrecy of the data. As far as the law of evidence is concerned, information systems will hardly be a major challenge, because there are few formalised rules on evidence in Norwegian law. Legislation may, however, be necessary or desirable to promote a wider acceptance of electronic transmission and storage of data. In some cases, references to paper-based transmission and storage in legislation that is not intended to prohibit electronic transmission and storage also call for the attention of the legislature.
PORTUGAL	Development of appropriate legislation in the areas of 1) the use of encryption systems; 2) digital signatures and electronic documents; and 3) the creation of Trusted Third Parties.	Protection of the intangible nature of goods, namely the security of information, will require a number of specific changes to current conventions regarding admissible evidence and the procedures for establishing proof. With regard to the criminalisation of offences and punishments severe enough to serve as effective deterrents, legislation faces two particular changes: 1) the potential consequences of certain breaches of security are such that a lack of proportion will inevitably arise between specific intent of the person committing the offence or his awareness of the consequences, and the potentially enormous scale of the damage, due to the fact that the offence is committed within an IT environment; 2) The precise classification of offences poses such problems that legislation, in defining certain criminal acts, has been forced to use rules which, despite being subject to formal proof, remain voidable. In view of this, there is a risk that courts might rule (under Article 29 of the Portuguese Constitution, which states that offences must be classified in the penal code) that such rules do not apply in certain cases.

SWEDEN	Legislation on digital signatures and electronic documents, establishment of Public Key Infrastructure and Certification Authorities, Trusted Third Parties for handling of secure communications.	The trustworthy replacement of paper documents by electronic documents in an open environment where partners are unknown to each other before deals are made.

	Q6. What policy measures might be taken in the future?	Q7. What are the most important challenges facing the legal system concerning security?
SWITZERLAND	Information vis-à-vis the general public needs to be improved. Also closer scrutiny needs to be given to the security of information systems.	In the legal framework for data protection the regulations set out the security objectives and basic preconditions which are relevant to all systems. The use of 'sensitive' information systems by Federal Government requires a legal basis. One of the most important challenges lies in finding a means whereby the regulations governing data protection can be measured.
UNITED STATES	It may be necessary to provide a legal foundation for some aspects of electronic commerce and security. These are being studied at many levels and by both the public and private sectors. The President's Commission on Infrastructure Protection will surely suggest policies to support the security of information systems.	The legal system faces a myriad of challenges regarding security issues in the use and management of information systems (see response to Q5). These challenges include 1) developing laws and practices regarding the creation and maintenance of transaction records which conceive information systems that support the security of the system and the privacy of its users; 2) developing identification mechanisms that similarly support both security and privacy; 3) determining jurisdiction over activity on networks, including the applicability of a given State's law, prosecutional jurisdiction; and 4) developing clear legal rules, acceptable to all States involved, regarding impermissible activities on networks.
UNITED KINGDOM	Future developments may include accredited certification against BS7799 and the introduction of licensing arrangements for Trusted Third Parties.	There are a number of challenges surrounding the greater use of electronic documents e.g. digital signatures, issues of IPR and those raised by an increasingly international environment.
INTERPOL (HELSINKI)	See answers to above questions.	The most important challenge is the legal anatomy of electronic documents.

IV. AWARENESS

	Q8. How would you describe the level of awareness?	Q9. What measures have been used to improve awareness?
AUSTRALIA	Current awareness is patchy although it has increased in the past few years, e.g. through the debate on Internet security. There has also been an increase in the number of attendees at security conferences. The awareness for broad issues like personnel and administrative security, and in areas associated with the Internet has not increased significantly.	Increase in the number of academic institutions offering IT security courses. This includes security courses designed for public sector employees. This scheme will be extended to the private sector in 1997. The OECD Guidelines have been referenced in several relevant standards.
AUSTRIA	The Security Guidelines have been presented to the commission of the government responsible for IT and made available to all ministries. A better evaluation of the awareness aspect was not possible due to lack of time.	
FINLAND	There is a broad awareness of the issues, although more needs to be done.	A translated version of the Guidelines has been used as training material.
FRANCE	The level of awareness in France is deemed higher than the European average (1992 study carried out by the European Commission's DGXIII).	Training and awareness courses for government agencies, trade associations and business enterprises have been intensified. These programmes make reference to the OECD Security Guidelines.
GERMANY	Security issues of information systems have become increasingly important for German society, including public, private, institutional sectors and the government. Subsequently the level of awareness has increased.	Those measures mentioned in the answers to Q1 and Q2 were used to improve awareness.
IRELAND	Awareness of security issues within the civil service is proportionate to the level of security of the information being processed. No information provided with regard to the private or public sector.	No activities took place to promote awareness of the Guidelines. All promotion activities have centred around the national guidelines and on general awareness of information security.
ITALY	It is not possible to reply to such a question without carrying out a specific survey and research of each organisation in the public and private sectors. It is generally understood that security is of importance in the public sector to the Ministry of Defence, Ministry of the Interior and the Ministry of the Presidency and in the private sector to the financial and banking organisations.	See answer to Q1.
JAPAN	User awareness of security issues is still not very well developed, although the risks are increasing (only 17 per cent of companies have full time security managers and only 14 per cent give training to their employees - survey by JIPDEC). In introducing new technologies (e.g. EDI, EFT) security has been recognised as an important matter. Recent incidents, e.g. the Hansin-Awaji earthquake, have raised the level of awareness. FISC has distributed the Guidelines.	Measures include: (i) Press release of the 1992 Security Guidelines, (ii) published reports and notifications about the Guidelines and other security matters e.g. by FISC (The Centre for Financial Industry Information Systems) in its periodical, (iii) establishment of the Japan Computer Emergency Response Team/Co-ordination Centre (JPCERT/CC), (iv) amendment of 'The Information Systems Security Guidelines', 'The System Auditing Guidelines' and 'The Computer Virus Prevention Guidelines', (v) promotion through seminars and workshops and (vi) collection of information about damages caused by computer viruses and unauthorised access.

	Q8. How would you describe the level of awareness?	Q9. What measures have been used to improve awareness?
KOREA	All sectors of society in Korea are very well aware of the importance of security issues.	Education for recognising the importance of security has been used to improve awareness of the Guidelines.
NORWAY	Awareness is overall uneven. Experts and some decision makers and politicians have high awareness. However, the majority of decision makers have low awareness, or if they are aware, they have little confidence in how to practically define and implement security policies.	Substantial effort has been undertaken in developing guidelines, arranging conferences, courses and other educational efforts in private as well as public sectors. The Norwegian Industrial Security Council has published a report "Datacrime - non registered figures, 1989-1992" (Norwegian title: "Datakriminalitet - m|rketall"), giving information and statistics about datacrime not being reported to Norwegian authorities during the time period. A new report for the time period 1993-96 is planned to be published shortly.
PORTUGAL	Following the dissemination of the OECD Guidelines, participation in the SOG-IS in 1992, the enactment of the legislation (see Q2) and from the initiatives in both the public and privates sectors, awareness has risen significantly.	Measures include 1) implementation of awareness campaigns and educational measures (courses, seminars and workshops); 2) publication and mass distribution of a "prospectus for technology diffusion" on "Security- an Imperative for Information Technology" which contains a series of recommendations on the use of IT by administrators, computer personnel and individual users; 3) publication and distribution of a technical manual, "Security of Information Systems and Technologies" by II and ANS; 4) publication and distribution of a Portuguese version of EC documents (see Q3) and the OECD Guidelines.
SWEDEN	Generally the situation is getting better. The major public and private organisations have much greater awareness than SMEs who are generally lagging behind.	The Guidelines have been made available to a large number of organisations and people in 1992/93. They were also referred to in the final report to the Ministry of Finance (report produced by the Government Co-ordination Committee on IT Security).
SWITZERLAND	Awareness of the importance of security issues is very varied both in the public and private sectors. The level of awareness is low. Only a small percentage of the population is taking an active interest in data security and protection issues.	Measures include: (i) passing of the Data Protection Law, Ordinances and policies and (ii) reports, press conferences etc. of the Data Protection Commissioner.
UNITED KINGDOM	Awareness of security issues is growing and there have been a number of activities to raise awareness. For example, the biannual 'Information Security Breaches Survey' which identifies both breaches and awareness of information security measures.	The development of BS7799 : A Code of Practice for Information Security Management has provided a base reference document to improve awareness. In addition, there have been a number of conferences and surveys which have also increased awareness.
UNITED STATES	See response to Q4. The level of awareness of security issues is certainly growing within both the US public and private sectors. Hearings were held in 1996 by the US Senate on the nation's vulnerability to what is often referred to as "information warfare." These hearings helped to increase public awareness.	Primary government measures have been the documents described in Q2. See also the responses to Q4 and Q8.
INTERPOL (HELSINKI)	Awareness is still not very high although it is increasing. The level of awareness is expected to increase over time as people learn the hard way by examples given of security incidents.	Response covered by answer to Q1.

V. INTERNATIONAL CO-OPERATION

	Q10. Has your country been involved in any efforts to improve international co-operation on information security issues?	Q11. What measures might be taken to improve international co-operation?
AUSTRALIA	At this stage, with the exception of protection of personal data and some elements of electronic commerce, information system security is a matter for users rather than governments. However, as technology evolves, unanticipated developments may require the implementation of international approaches as occurred in the case of cryptography. Often these unanticipated developments crystallise as a result of discussions in forums such as the OECD. There would be a role for OECD in bringing together Member countries to discuss developments and their potential implications.	
AUSTRIA	Through the membership of the European group SOG-IS (Senior Official Group - Information Security).	The OECD could co-ordinate its work with that of the EU and create a forum where non-EU States can voice their concerns.
FINLAND	No specific activities were given in response - see answer to Q 3.	International work on information security issues could be focused through the activities of the OECD.
FRANCE	Involvement in the following activities: (i) OECD Ad Hoc Group of Experts on Cryptography Policy Guidelines; (ii) ISO/IEC JTC 1/SC27 Security Techniques; (iii) formulation and standardisation of Common Criteria for evaluating and certifying information technologies; (iv) EU activities including various 'think tanks' on the security of information systems.	The OECD can be used to test the relevance and formulation of principles before they are made directly applicable or binding within another framework.
GERMANY	Close contact and involvement with: (i) international partners, government and industry, on IT security issues; (ii) formulation of European evaluation criteria ITSEC and the international Common Criteria.	OECD has a future role with regard to security issues and international co-ordination, as demonstrated by the current work on Cryptography Policy. The OECD could act as a forum for discussing security issues.
IRELAND	Involvement with the European project EPHOS including the part dealing with information security.	Work on specific security issues should be dealt with (e.g. security of transnational transactions) rather than assume that because a solution works in one country it will work in other countries.
ITALY	No.	The OECD could play an important role in improving the level of awareness of the governments and the private sector with regard to the security of information systems. It would nevertheless be necessary to set up a proper permanent observatory within the OECD, as already called for by many countries, including Italy.
JAPAN	Involvement in: (i) international conferences on information security issues including the OECD conference on 'Security, Privacy, Intellectual Property Protection in the GII', and (ii) proposed joint study on telecommunications technology for use in networks which are able to resist disasters.	OECD activities such as those facilitating international discussion, debate and information exchange are very important in this respect. FISC in Japan is prepared to facilitate exchange of information relating to the Guidelines and their implementation.
KOREA	Involvement in the OECD ICCP Committee and expert meetings.	As a new member of the OECD, the Korean government is going to exercise their best efforts in this area.

	Q10. Has your country been involved in any efforts to improve international co-operation on information security issues?	Q11. What measures might be taken to improve international co-operation?
NORWAY	Norwegian Government representatives, backed by, and in consultation with the Norwegian authorities and industry representatives, are participating in (i) the ongoing work on crypto guidelines in OECD, and (ii) the EC's SOG-IS. Norway Post has, together with the Nordic postal agencies in Sweden, Finland and Denmark, developed a common system based on open and international standards (X 509) and smart cards, and will introduce new security services for electronic messaging and electronic commerce. It will be the first open international security service. The name of the service is Nordic Post Security Service (NPSS). The Postal Agencies of several other countries have shown interest in the system, and International Data Post (IDP) are now developing a common security profile which all members of IDP (16 countries) can use as a basis for their own solutions. European security projects in the health care sector include: (i) INFOSEC '94 programme (project THIS), (ii) the Health telematics programme (4th framework, project TrustHealth) and (iii) work in CEN TC251 (Medical informatics) WG6. In 1993 the Nordic Council of Ministers produced a report on "Information Security in Nordic Countries".	The ongoing work on crypto guidelines is important. Also guidelines on the further development of the legal system may need to be considered, e.g. the recent German law on digital signature, and the UN "draft model statutory provisions on the legal aspects of electronic data interchange (EDI) and related means of data communications".
PORTUGAL	Participation in SGO-IS.	Broader and more effective co-ordination with international institutions, such as SOG-IS with EC DG XIII.
SWEDEN	Involvement in EU and OECD activities.	OECD could concern itself with the international recognition of digital signatures and propose appropriate measures.
SWITZERLAND	Participation in the Council of Europe with regard to data protection questions. Also involved in (i) international conferences of the Data Protection Commissioners and (ii) co-operation with the OECD.	The OECD has an important role to play in the improvement of international co-operation with regard to the security of information systems.
UNITED KINGDOM	Involvement in international co-operation in a number of fora including activities of the European Commission, international standards bodies and with industry groups.	The OECD provides a useful fora for discussion and international co-operation on information security issues.
UNITED STATES	Besides work with the OECD on cryptography guidelines, the US participates in ISO, IEEE and many other international standards bodies which address security. The US has also been actively involved in the Common Criteria effort, which is a multi-national effort (the US, Canada, France, Germany, the Netherlands and the UK) to develop a structure for the description and evaluation of security-related products. The first draft of the Common Criteria was issued in January 1996. The US also participates in discussions on computer crimes issues at the Council of Europe and the P8.	In order to provide a secure and reliable foundation for global electronic commerce, international co-operation on public key infrastructure functions may be appropriate.

	Q10. Has your country been involved in any efforts to improve international co-operation on information security issues?	Q11. What measures might be taken to improve international co-operation?
INTERPOL (HELSINKI)	Involvement in many activities to improve international co-operation. The five most important activities are: (i) ICPO - Interpol, (ii) OECD, (iii) Council of Europe, (iv) United Nations and (v) SOG-IS.	Among the measures to be taken are joint ventures to enforce the OECD 'Multidisciplinary Principle'. There is a future role for OECD to build an international framework for IT security.

VI. REVISION OF THE GUIDELINES

	Q12. Are the 1992 Guidelines still adequate?	Q13. Should the Security Guidelines also cover information security?	Q14. Would the 1992 Guidelines be more useful in a different format or at a more detailed level?	Q15. Is there a need for a set of Guidelines with a wider scope?
AUSTRALIA	While there have been significant technological advancements in the past five years, the basic objective and principles of the 1992 Guidelines are still relevant. There may be a need to review the application of the principles in the new environment.	The convergence of technologies has resulted in an overlap of issues relating to security, privacy, intellectual property protection of consumer issues, government revenue generation, law enforcement and electronic commerce. Rather than replacing existing guidelines, they should be reviewed and an overarching set of principles developed which will ensure a consistent approach to the different issues.		
AUSTRIA	The security of wireless communications and interconnecting networks, especially the Internet, must be addressed. This should cover subjects such as firewalls, e-mail, file transfer technology, on-line telephony and general improvements in the security infrastructure for telecommunications.	This requires a definition of 'information security' to avoid conflict with the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and with aspects considered in the new OECD Cryptography Guidelines.	A more detailed set of guidelines might be appropriate to create compatibility in key areas. The OECD should strive to identify these areas.	The question could not be answered because internal discussion was not possible.
FINLAND	For the most part, the Guidelines are still adequate and no major revision needs to be undertaken. However, the Guidelines and the Memorandum, should be amended and extended to cover networking and related aspects (see answers to Q5 and Q7).	If the term 'information security' has a broader meaning than 'security of information systems', e.g. it covers information in networks, then the answer is yes.	The present format is satisfactory.	See answers to Q12 and Q13.

	Q12. Are the 1992 Guidelines still adequate?	Q13. Should the Security Guidelines also cover information security?	Q14. Would the 1992 Guidelines be more useful in a different format or at a more detailed level?	Q15. Is there a need for a set of Guidelines with a wider scope?
FRANCE	The Guidelines are still relevant and require no overall revision.	The Guidelines should not be extended to cover information security. This is a matter for individual States, and public and private parties to consider, and which is covered by separate legal provisions. See additional supporting comments provided by France.	The current format and level of detail seem to be perfectly readable and applicable. Also any changes to the Guidelines would have an impact on the initiatives undertaken since they were published.	No, the present Guidelines seem to satisfy current requirements.
GERMANY	The Guidelines still appear to be adequate insofar as it is not deemed necessary to create an entirely revised set of guidelines.	This question can only be answered if the term 'information security' is clearly defined.	The format and level of detail of the 1992 Guidelines seem to be adequate.	At the moment, there seems to be no need for a set of guidelines with a wider scope than those of 1992. This position could be altered in the case where the future Guidelines on Cryptography Policy and the OECD deliberations in the field of GII have a strong influence on security issues.
IRELAND	The OECD Guidelines are written at such a high level of abstraction as to be of marginal use in implementing day-to-day security solutions. While they do provide a possible framework for the implementation of information security such frameworks could equally be provided at the national level.		As for future developments, it is unlikely that, due to differences in priorities and requirements, a sufficiently detailed set of guidelines, both relevant and implementable at national levels, can be written at the international level. Also there is little benefit in duplicating the work of other fora such as the EPHOS project or the work of EWOS.	
ITALY	When reviewing the 1992 Guidelines it will be necessary to take into account the development of computer networks and in particular the Internet, and the new security problems arising from such a development.	Information security cannot be covered by the present Guidelines. It would be necessary to proceed to a broader type of work which would probably lead to a different type of recommendation.	Yes.	Yes. The development of technology requires a periodic revision of the Guidelines in order to face the new problems of information security. In any case it would be necessary that governments reach formal agreements aimed at setting up multilateral international instruments. In practice, we need to create a proper international legal system concerning information security.

	Q12. Are the 1992 Guidelines still adequate?	Q13. Should the Security Guidelines also cover information security?	Q14. Would the 1992 Guidelines be more useful in a different format or at a more detailed level?	Q15. Is there a need for a set of Guidelines with a wider scope?
JAPAN	The general concept of the Guidelines is still effective. However, as the scope of security issues has widened and the use of networks is increasing, the OECD should consider enhancing the Explanatory Memorandum of the 1992 Guidelines to adapt to these circumstances. Some revision of the Guidelines may be needed in the future.	A definition of the term 'information security' needs to be given. The definition of 'information system' is comprehensive and as such issues related to information security can be included in the Guidelines. For example, computer virus protection could be included in the Guidelines.	The Guidelines should provide general principles rather than go into details. Hence the current format and level of detail is adequate. Discussion at a more detailed level should be discussed separately, if necessary.	It is unnecessary to produce a new set of Guidelines with a wider scope since the current set cover almost all basic security ideas and they are still effective.
KOREA		Information security is an important part of information systems. Therefore, information security should be covered in the Guidelines.	The Guidelines should be integrated with related guidelines such as the 1980 Privacy guidelines. It would also be useful to provide more details.	Information security is closely related to the security of information systems, and cryptographic methods play an important role in information security. Therefore, the integration of all Guidelines is useful for security and safety of information systems.
NORWAY	The 1992 Guidelines could eventually be extended to include TTP and digital signatures, but this should be carefully discussed. Alternatively, separate guidelines on these topics could be considered.	In order to answer this question, the concept of information security should be defined relative to the concept of information systems security.	A different format of the existing Guidelines is not needed. Developing more detailed guidelines may be discussed, e.g. the US-based "Generally accepted System Security Principles (GSSP).	A preliminary answer to this question should follow as a consequence of the answers to some of the questions above. This answer could be discussed at working party level.
PORTUGAL	The Guidelines need to be revised to take into account the massive increase of use of the Internet.	Yes.		No.
SWEDEN	The Guidelines are still adequate.	The Guidelines should not cover information security.	Difficult to say.	No. Sweden has no precise ideas or proposals to make in this area.
SWITZERLAND	The Guidelines are still adequate, but it would be good if they could be improved.	The Swiss believe that the term 'information security' also covers the term 'security of information systems'.	A set of Guidelines at a more detailed level would be appreciated.	See answers to Q12 and Q14.

	Q12. Are the 1992 Guidelines still adequate?	Q13. Should the Security Guidelines also cover information security?	Q14. Would the 1992 Guidelines be more useful in a different format or at a more detailed level?	Q15. Is there a need for a set of Guidelines with a wider scope?
UNITED KINGDOM	The principles outlined in the OECD Guidelines remain adequate.	If the Guidelines were to be reviewed then this would be an opportune time to consider whether they should apply to information security and to consider their relationship to aspects of data protection and privacy.	The principles of the guidelines are consistent with a range of more detailed guidance and the UK sees no reason why the guidelines should be revised in this area.	See answers to Q13 and Q14.
UNITED STATES	The core concepts introduced in the Guidelines are still sound and the Guidelines have been well received in the US. However, the language could be simplified and clarified e.g. the elements of computer security written by NIST attempt to describe the principles in a less technical way in order to be easily understood.	We do not quite understand the questions as the Guidelines specifically address the confidentiality, integrity and availability of "information".	See response to Q12. The Guidelines are in need of revision to improve their clarity. It may also be useful to provide 5-10 suggestions for implementing each principle, although the difficulty of doing so should not underestimated.	There is insufficient evidence to suggest the new Guidelines are necessary. We would recommend that the Secretariat analyse the answers submitted in response to this questionnaire by all Member countries before attempting to assess the need to replace the 1992 Guidelines.
INTERPOL (HELSINKI)				