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

24-Sep-2004

English - Or. English

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

DSTI/ICCP/REG(2003)8/FINAL
Unclassified

Cancels & replaces the same document of 17 June 2004

Working Party on Information Security and Privacy

SUMMARY OF RESPONSES TO THE SURVEY ON THE IMPLEMENTATION OF THE OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: TOWARDS A CULTURE OF SECURITY

www.oecd.org/sti/security-privacy

JT00169904

English - Or. English

FOREWORD

This report sets out the results of responses received from 22 member countries to the *Survey on the Implementation of the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, which was issued in July 2003. It is intended to provide an understanding of the implementation initiatives in place within member countries.

The report was prepared by the OECD Secretariat with active input and comments from member countries. It was declassified by the Committee for Information, Computer and Communications Policy on 10 June 2004.

This report is published on the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

SUMMARY OF RESPONSES TO THE SURVEY ON THE IMPLEMENTATION OF THE OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: TOWARDS A CULTURE OF SECURITY

Purpose and objectives

Considering that a co-ordinated action plan is essential for the effective implementation of the 2002 *OECD Guidelines for the Security of Information Systems and Networks* ("Security Guidelines"), OECD member countries adopted the "Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security"[1] ("OECD Implementation Plan") and released it to the public in January 2003. A survey questionnaire [DSTI/ICCP/REG(2003)7] was circulated to OECD member countries in July 2003 to take stock of initiatives they had undertaken since the release of the Security Guidelines in August 2002, as consistent with the OECD Implementation Plan.

Survey structure and content

The survey questionnaire followed the structure of the OECD Implementation Plan.

It included 24 questions related to:

Part I. The roles of government

A. Government responsibility for public policy
B. Outreach and support for other participants
C. Government as owner and operator of information systems and networks
D. Government as user of information systems and networks

Part II. The roles of business and civil society

A. Business as owner, operator and/or user of information systems and networks
B. Civil society as users of information systems and networks.

The survey questionnaire was circulated to member countries for completion by mid-August 2003. For the benefit of comparison, responses were to reflect progress made through 31 July 2003.

The Working Party on Information Security and Privacy agreed at its 15th meeting on 15 October 2003 in Oslo that by 14 November 2003 member countries that had not yet responded to the survey would do so and that member countries that had responded to the Implementation Survey would review the interpretation of their input and send their changes to the Secretariat. Since then, the Secretariat has received eight additional answers from member countries. In addition, two member countries have updated their answer to the survey. The information received has been incorporated in this document.

The list of the survey questions is found in Annex A.

Survey responses

Responses were received from 22 member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Hungary, Italy, Japan, Korea, Mexico, Netherlands, Norway, Portugal, Slovak Republic, Spain, Sweden, United Kingdom and the United States.

Most questions in the survey were phrased in an open way and comments were invited as appropriate. Due to variation in responses by member countries, the responses provided a series of illustrative examples, rather than an exhaustive list, of national initiatives. The general observations below, as well as the summary of responses, are to be read as an *interpretation* of the information provided.

General observations

Generally speaking, responding countries have effectively undertaken to provide leadership in developing a culture of security. Indeed, a very high number of positive responses were provided to most of the questions which asked member countries whether or not they had taken action, consistent with the OECD Implementation Plan. The detailed answers provide illustrative examples of measures or programmes of interest for effectively implementing the Security Guidelines. The exercise is also useful in terms of identifying areas which have received a high level of attention and areas in which member countries could strengthen their efforts. These results can be used by the Working Party on Information Security and Privacy (WPISP) to develop an action plan to further foster the development of a culture of security and establish priorities for the various elements of the plan.

High degree of attention

Respondents appear, thus far, to have placed the highest degree of attention on the development or amendment of a national policy framework, and on the implementation of the policy principles of the Security Guidelines, in particular the “Awareness” and “Response” principles.

- ***National public policies***
  - **All** responding countries have developed a national policy for the security of information systems and networks or are in the process of developing one. **All** respondents recognise and use the Security Guidelines as a reference policy framework.
  - **Most** responding countries have enacted a comprehensive set of measures to combat cybercrime.

- ***Awareness raising, education and training***

  These appear to be the first areas of focus for member countries with regard to implementing the Security Guidelines.
  - **All** respondents except one are active in awareness raising and many have hosted conference-type events, launched Web sites and released publications.
  - **Several** countries mentioned interesting initiatives, such as creating an IT security professional certification programme and the corresponding training or targeting of top management and new employees.
  - **Some** countries have targeted specific populations such as young people, the general public, IT (information technology) professionals or small and medium-sized enterprises (SMEs).

- ***Computer Emergency Response Teams (CERTs)***
  - **Most** responding countries support the establishment and use of CERT-like sites. Some report the establishment of CERTs for government, or CERT initiatives targeting SMEs and/or the general public.

Lower degree of attention

Respondents appear to have placed, thus far, a lower degree of attention on:

- ***Best practices***
  - **Many** responding countries have reported programmes to foster the development and sharing of best practices.
- ***Partnerships among participants***
  - **A few** responding countries have reported the establishment of public/private partnerships to address the security of information systems and networks.
- ***Standards***
  - Even though the use of international standards was not specifically addressed in the survey questions, **a few** countries mentioned ISO/IEC 15408[2] and/or ISO/IEC 17799/BS7799[3] as tools used for setting rules for government IT purchases, or assessing compliance of government systems with "Risk assessment", "Security design and implementation", "Security management" and "Reassessment" principles of the Security Guidelines.

Need for further information

- ***Oversight of the use of information systems and networks***
  - Responses as to how member countries ensure that their use of information systems and networks is consistent with the Security Guidelines were fairly general. **The majority** of the responses referred to the establishment of a national policy for the security of information systems and networks or of security guidance consistent with the Security Guidelines. **Several** referred to a national body responsible for following and/or checking the implementation of IT security policies. **One country** reported the requirement of an annual independent audit for all agencies. Further details on the means used by member countries to ensure consistency of the use of information systems and networks with national policy and the Security Guidelines might be of interest for future activities concerning the implementation of the Security Guidelines.
  - Information on the impact of the initiatives undertaken was not requested as such (*e.g.* number of paper copies of the Security Guidelines printed and/or distributed, or number of downloads for the electronic version; or number of people targeted by awareness-raising campaigns, and how many were reached and what measurable impact the initiative generated). It might be interesting to obtain such information for future research on the implementation of the Security Guidelines.

Possible actions to further foster the development of a culture of security

Next steps to be considered by the WPISP could aim at further monitoring and co-ordinating a consistent implementation of the Security Guidelines in order to boost the development of a global culture of security. A priority could be to strengthen global co-operation and collaboration in the areas that have thus far received lesser attention, and to foster the exchange of practical experiences and best practices among participants, as well as with non-member economies. As an example, member countries could undertake to explore further their implementation of the nine principles of the Security Guidelines. A greater level of detail on the implementation of the "Security management" principle (or security life cycle principles) of the Security Guidelines would facilitate the sharing of information on practices, measures and procedures at the practical level. Member countries could also decide to allocate more time and resources to enrich and maintain the information provided on the OECD Culture of Security Web site.

Possible means to accomplish the above could include further reporting and data collection activities, carrying out fact-finding missions or organising educational peer-reviews. The latter would request that the WPISP decide how to proceed with regard to: *i)* the basis for proceeding; *ii)* the agreed set of principles, standards and criteria against which a country policy and practices would be reviewed; *iii)* the designated actors to carry out the peer review exercise; and *iv)* the set of procedures to achieve the final result of the educational peer review.

Summary of responses

This summary includes a short paragraph of interpretive comment *(in italics)* followed by factual elements, by survey question.

I. Roles of government

Dissemination and translation of the Security Guidelines (Q1-Q3)

All responding countries have taken action to disseminate the Security Guidelines, mainly through traditional distribution channels such as hard copies, electronic transmissions or posting on Web sites. Few countries mentioned having made the Security Guidelines publicly available through press releases, television or production of CD-ROMs. In addition to the French and English versions of the Security Guidelines, the guidelines are available in eleven languages.

Means for public dissemination of the Security Guidelines include:

- Hardcopies: Australia, Canada, Czech Republic, Denmark, Finland, Hungary, Japan, Korea, Mexico, Netherlands, Norway, Sweden, United Kingdom, United States.
- Electronic copies: Australia, Austria, Belgium, Canada, Czech Republic, Finland, Hungary, Italy, Japan, Korea, Mexico, Netherlands, Norway, Portugal, Slovak Republic, Sweden, United Kingdom.
- Links to the OECD Web site or files on their national Web sites: Austria, Canada, Czech Republic, Finland, France, Germany, Hungary, Italy, Japan, Korea, Mexico, Netherlands, Norway, Portugal, Spain, Sweden, United Kingdom, United States.

- Related information on national Web sites together with either a link or the full text of the Security Guidelines: Australia (Q&A fact sheet), Austria, Belgium, France (guide book on the Security Guidelines), Hungary, Norway, Portugal, Japan, United States.
- Other means: Germany, Sweden and United States (press release), Japan (press release, television appearance, brochures), Mexico (e-government network).

With regard to translation, the Security Guidelines have been made available in 12 languages, covering almost all responding countries' languages: Czech, Dutch, Finnish, German, Hungarian, Italian, Japanese, Korean, Norwegian, Portuguese, Slovak and Spanish. A Swedish translation is forthcoming.

A. Government responsibility for public policy

National policies (Q4, Q5)

All responding countries have developed a national policy for the security of information systems and networks or are in the process of developing one. National policies on security of information systems and networks often include a specific framework for the security of government information systems and networks or protection of critical infrastructures. All respondents recognise and use the Security Guidelines as a reference policy framework. In terms of priorities, a few respondents mentioned the establishment of a culture of security, research and development and international co-operation.

Responding countries report that they have:

- Developed a national policy for the security of information systems and networks as part of a broader national policy on the information society: Australia, France, Japan, Netherlands.
- Developed a specific national policy for the security of information systems and networks: Finland, Hungary, Korea, Norway.
- Have specific policy frameworks for the security of their government's information systems and networks: Austria, Canada, Finland, Japan, Italy, Spain, United Kingdom; and/or for the protection of critical infrastructures: Australia, France, Japan, United Kingdom, United States.
- Are in the process of developing a national policy: Belgium, Czech Republic, Denmark, Portugal, Slovak Republic, Sweden, or have such a policy as a project for the future: Germany.

All responding countries recognise the Security Guidelines as a reference policy framework. Along with the Security Guidelines, Denmark mentioned the European Union (EU) policy documents on information systems and network security.

Australia has reported support initiatives within the Asia-Pacific Economic Cooperation (APEC) and other forums to assist with the implementation of the Security Guidelines, for example by helping the development of the APEC Cybercrime Legislation and Enforcement Capacity Building Project.

Measures to combat cybercrime (Q6, Q7)

Most responding countries have enacted a comprehensive set of measures to combat cybercrime. In decreasing order, the most frequent measures taken by the large majority of responding countries are: the identification of national cybercrime units; initiatives to set up a CERT-like institution; initiatives to set up international high-technology assistance points of contact; specific measures for the collection of evidence of cybercrime, and the development of closer co-operation between law enforcement organisations and

business about the security of information systems and networks. These measures are generally as comprehensive as, and consistent with, the Council of Europe Convention on Cybercrime.

Measures to combat cybercrime include:

- Identification of national cybercrime units: Australia, Austria, Belgium, Czech Republic, Finland, France, Germany, Hungary, Italy, Japan, Korea, Mexico, Netherlands, Norway, Spain, Sweden, United Kingdom.
- Specific measures on the collection of evidence of cybercrime: Australia, Austria, Belgium, Finland, France, Germany, Italy, Mexico, Netherlands, Norway, United Kingdom, United States. Japan is preparing such measures. The Korean Cyber Terror Response Center (CTRC) monitors Web sites that provide illegal adult material.
- Legislative measures such as preservation of traffic data in order to support law enforcement activities to deal with cybercrime: Australia, France, Italy, Netherlands, United Kingdom. Finland, Japan and Korea are preparing such measures. Swedish legislation provides for voluntary retention of traffic data by ISPs up to 12 months.
- Initiatives to set up institutions, whether public sector or private sector, that exchange threat and vulnerability assessments [such as national CERTs (Computer Emergency Response Teams)]: Australia, Austria, Belgium, Canada, Finland, France, Germany, Hungary, Italy, Japan, Korea, Mexico, Netherlands, Norway, Spain, Sweden, United Kingdom.
- Co-operation between government and business in the fields of security of information systems and networks and fighting cybercrime, including agreements between law enforcement organisations and business about the security of information systems and networks: Austria, Australia, Finland, Germany, Italy, Japan, Korea, Mexico, Netherlands, Norway, Sweden, United Kingdom.
  - Co-operation with business regarding protection of critical infrastructure: Australia, Japan.
  - Collaboration with ISPs (Internet Service Providers): Austria, Germany, Korea, Mexico.
  - Co-operation with business in an “Information Security Council”: Sweden.
- Designation of international high-technology assistance contact points: Australia, Austria, Finland, France, Germany, Italy, Japan, Korea, Mexico, Netherlands, Norway, Sweden, United Kingdom, United States. Belgium is discussing the creation of such points of contact.
- Other initiatives related to international co-operation:
  - Mutual assistance agreements: Australia, United States.
  - Participation in the APEC Telecommunications and Information Working Group, provision of training to non-member countries: Australia.
  - Policy measures and tools developed by agencies to increase cross-border co-operation such as databases to help better identify cases of fraud: United States.

The Czech Republic mentioned that it will join the EU programme, Safer Internet Action Plan,[4] by accession to the European Union in May 2004.

National measures mentioned above are considered by responding countries as comprehensive, and consistent with, the Council of Europe Convention on Cybercrime. Finland, Norway, Portugal and Sweden are currently in the process of amending their legislation to make it consistent with the Convention.

B. Outreach and support for other participants

Awareness raising (Q8)

All responding countries except one report initiatives that aim at awareness raising. Conference-type events, Web sites and publications are most frequently mentioned. Among other interesting initiatives, more than 1 million CD-ROMs have been distributed through magazines and via preinstalled material on new computers. Several countries have also reported initiatives aimed at targeting specific populations, including the general public and newcomers to IT, SMEs, and young users. One country issued a special "Donald Duck" cartoon magazine on safe Internet usage, and another created a portal on security of information systems and networks for SMEs.

Awareness-raising initiatives include:

- Workshops, seminars, training, conferences, and associated papers and studies: Australia, Czech Republic, France, Germany, Hungary, Japan, Korea, Mexico, Netherlands, Portugal, United States.
- Web site(s) and portal(s): Australia, Finland, France, Germany, Japan, Korea, Netherlands, Portugal, Spain, Sweden, United Kingdom, United States.
- Publications, guides, manuals and brochures: Australia, Denmark, Finland, France, Germany, Netherlands, Sweden, United States.
- Mass media: Finland, Korea, Netherlands, United States.
- CD-ROMs: Germany.
- Guidelines/recommendations, methodologies, best practices: Finland, France, Hungary.
- Involvement in associations, federations, societies (such as the *Fraunhofer Institute*): Germany.
- Creation of a committee to enhance awareness: Italy.
- Newsletters: Netherlands.
- Telephone hotlines: United States.
- "Idea contest for the security of information systems and networks" for the general public: Korea.
- "Roadshows": Australia.
- In the context of implementing their e-government programme Austria will launch a "trust and security" initiative in 2004.
- The Slovak Republic has not developed programmes and initiatives in this field up to now.

Several respondents have developed products targeting specific populations:

- Citizens and new IT and Internet users: Germany (the content of a Web site is also preinstalled on Fujitsu-Siemens new personal computers), Japan, Netherlands, Sweden, United Kingdom, and the United States (end-user oriented Web sites).
- Business: Canada has presented the Guidelines during the drafting and following the adoption to the members of the Information Technology Association of Canada (ITAC) which represents 1 300 companies in the information and communications technology industry and consults with various industry associations on security related issues.

- SMEs:
  - Australia produced a special package of information resources and a security portal.
  - The Netherlands published a security guide for SMEs.
  - Sweden has made information on Internet security (Web site and printed material) available targeted at SMEs.
  - The UK government has a partnership with industry, "UK Online for Business".
  - The US Computer Security Resource Center has a Small Business Initiative.

- Young people: Germany launched a targeted Web site; the Netherlands sponsored a special issue of the "Donald Duck" cartoon magazine on safe Internet usage. Korea launched a Slogan/Poster Contest for elementary/middle/high school students on the security of information systems and networks.

Various agencies/ministries are tasked with organising awareness-raising initiatives, for example: the Council for IT Security (Denmark), the Ministry of Finance (Finland), the Federal Office for Information Security (Germany), the National Police Agency (Japan), the Ministry of Trade and Industry and Ministry of Justice (Norway), the Ministry of Science and Technology (Spain), the Federal Trade Commission (FTC, United States) and National Institutes of Standards and Technology (NIST, United States).

Best practices and partnerships (Q9, Q10)

Many responding countries have programmes to foster the development of best practices and partnerships among participants. Among others, an interesting initiative was reported that awards business "best practices for the security of information systems and networks". Most respondents also support the exchange of best practices to improve users' abilities to understand and implement effective and up-to-date security measures. Examples include participation in, and/or sponsoring of, workshops and working groups. Establishment of public-private partnerships and use of standards are mentioned by a few countries.

Programmes to foster the development of best practices include the following examples:

- Developing and/or publishing best practices or recommendations: Austria (public sector), Finland, France, Germany, Hungary, Korea, Norway, United States.
- Establishing public/private partnerships to bring together participants and experts from various areas to work on how to minimise the risks of using the Internet (Netherlands) or to provide SMEs with impartial advice about e-business and information communication technology (ICT) (United Kingdom). Partnering with groups and consortia and sponsoring of the Programme Managers' Forum for the security of information systems and networks to address issues of mutual concern (United States).
- Creating a programme to award business "best practices for the security of information systems and networks" and of a committee for security of information systems and networks practice to promote partnerships among participants: Korea.
- Creating a group to bring together cybercrime specialists of the different offices of the federal government, services providers, business and educational institutes: Mexico.
- Establishing a Business-Government Task Force on Critical Infrastructure: Australia.

The exchange of best practices is supported through the means listed above as well as through the creation of Web sites (Korea, United Kingdom, United States), organisation of workshops and seminars (Finland) and sponsorship (United States).

As regards international standards, the United Kingdom provided the Secretariat for the BS7799/ISO 17799 Users' Group. The Japanese government has established an evaluation and certification scheme based on ISO/IEC 15408 to help IT users procure secure information systems and products. It has also established the Management Systems Conformity Assessment Scheme and an Auditing System for the security of information systems and networks (both based on ISO/IEC 17799) in order to enhance management of the security of information systems and networks. The Swedish Agency for Public Management has published guidelines in support of 24/7 agencies with advice on how to use SS-ISO/IEC 17799. Spain has financed studies regarding the use of ISO/IEC 17799 in Spanish enterprises.

The United States mentioned the existence of guidelines developed by trade associations, such as the Business and Industry Advisory Committee (BIAC), Business Software Alliance (BSA) and Information Technology Association of America (ITAA).

Denmark will focus on best practices in the future. The Slovak Republic has up to now no programmes for the development and exchange of best practices.

Education and training (Q11)

All respondents except one support education and information programmes on the security of information systems and networks. Several countries mentioned interesting initiatives, such as creating an IT security professional certification programme and the corresponding training or targeting of top management and new employees. Except for one example,[5] no practical illustration of the implementation of the "ethics" and/or "democracy" principles in education or training was provided.

In addition to the tools mentioned under awareness-raising, educational programmes concerning the security of information systems and networks, material or toolkits include:

- Initiatives to include security of information systems and networks in educational programmes for top management and new employees: Finland.
- Guides and corresponding training for IT security: France, Germany.
- IT security professionals certification programme and corresponding training: Japan.
- Support for the qualification "Network Information Security Manager" for IT professionals: Japan.
- Support for an annual workshop which discusses current trends in foreign countries' education regarding security of information systems and networks, and for the standardisation of mid-/high-education institute's curricula and the future of education on security of information systems and networks; "Study Material Contest" for elementary/middle/high school teachers in preparation to provide for a standard curriculum on security of information systems and networks: Korea.
- Educational packages for elementary and middle schools and measures to incorporate teaching of security of information systems and networks at university and college levels in areas such as health and business management: Norway.
- Promoted the upgrade of the secondary school programme in order to increase awareness and knowledge of junior students in the ICT field: Portugal.

- Online Security "Health Check" tool: United Kingdom.
- Making a dictionary on security of information systems and networks encompassing about 1 000 definitions and their interpretations available on the Internet: Hungary.
- Public/private partnership: United States (GetNetWise – this Web site focuses on online security and privacy).
- Hungary is preparing to survey the educational field of informatics and the extension of the technical training with aspects of security of information systems and networks. Supplementary material on the security of information systems and networks for educational purposes and related examination criteria will be developed. Regular, compulsory IT security training for IT experts and system administrators working for government agencies is also in preparation.
- France has put in place an education centre for the public administration.
- Spain supports different educational programmes on the security of information systems and networks, both at the basic computer education level and for postgraduate studies.
- Belgium has issued minimum guidance on protection against viruses as a starting point for the development of education and awareness measures by the future Belgian agency for the security of information systems and networks.
- The Slovak Republic has up to now not supported education and information programmes on the security of information systems and networks.

Denmark's programme for IT security focuses on education, but no specific awareness and training programme has yet been launched.

Computer Emergency Response Teams (CERTs), SysAdmin, Audit, Network, Security (SANS), Information Sharing and Analysis Centres (ISAC) and other useful sites[6] *(Q12)*

Most responding countries support the establishment and use of CERT-like sites. Some report the establishment of CERTs for government, or CERT initiatives targeting SMEs and/or the general public. A few countries mentioned the establishment of a structure similar to ISAC or indicated some interest in doing so. No country made a specific reference to SANS-like sites. Initiatives to foster international co-operation in this area are mentioned by fewer countries.

As regards CERT-like sites, responding countries report the following:

- Implementation of or co-operation with CERT-like sites: Australia, France, Germany, Hungary, Mexico, Norway, Portugal, Spain, Sweden, United Kingdom.
- Implementation of a government-specific CERT: France, Italy (in progress), Korea, Netherlands.
- Implementation of CERT-like services targeting specific populations: Korea (the general public, IT experts), Netherlands (SMEs), Korea. As an example, Netherlands' National Warning Service for viruses and computer-security-related incidents warns the general public and SMEs by publishing alerts on a Web site and via e-mail and SMS messages, depending on how critical the problem is. A hotline helps users to report incidents.
- Legislation in preparation to make it mandatory to inform CERT of serious infringements of the security of information systems and networks: Finland.

- Discussion in progress about the creation of a Computer Security Incident Response Team (CSIRT) as part of the future national agency for the security of information systems and networks: Belgium.
- Support for CERTs co-operation in the Asia-Pacific region: Japan.
- Support for a variety of initiatives at the international level (*e.g.* APEC, OECD, G8) and with the private sector: United States.

As regards ISACs-likes sites, Australia has supported the establishment of sectoral Infrastructure Assurance Advisory Groups to facilitate information sharing between owners and operators of critical infrastructures. Japan supports a "Telecom ISAC". The Austrian Government is a partner to the "Computer Incidents Response Coordination Austria (CIRCA)" formed by network and security officers of ISPs and other network providers (public and private). Germany mentions that even though it has no ISAC-like mechanism, competent agencies are endeavouring to further promote relevant co-operation between government and industry.

The creation of the European Network and Information Security Agency (ENISA) at the EU level has also been mentioned as a possible important player regarding information on the security of information systems and networks.

Research and development (Q13)

Most responding countries support research and development (R&D) to increase security, but the means to achieve this support vary from country to country. A more frequent use of R&D programmes and of hardware, software and auditor certification is found, however.

Government support for R&D includes:

- R&D programmes: Australia, France, Czech Republic, Denmark, Hungary, Japan, Korea, Netherlands, Norway, Spain, United Kingdom. For example, Netherlands' Sentinel long-term R&D programme aims at contributing to a comprehensive framework for secure systems engineering and networking.
- Hardware/software certification: France, Italy, Sweden.
- Auditor certification: Germany.
- Cryptographic systems and hardware and software solutions, *e.g.* targeting SMEs: Germany.
- Tax system for R&D support: Japan.
- Legislation to reinforce the importance of R&D to improve security and foster best practices: United States.
- Founding and financing of the "Austrian Center for Secure Information Technology" (A-SIT) for monitoring and conducting research on security technologies and security threats: Austria.

R&D is supported by Mexico to increase best practice operational procedures. Finland has no special stand-alone support for R&D on security of information systems and networks, but innovation is supported through its more general support framework.

C. Government as owner and operator of information systems and networks

Policy on security management of governments' own systems and networks (Q14, Q15, Q16)

Nearly all responding countries have developed a policy, standards, recommendations, or manuals on security management for their government's own systems and networks. Among others, an interesting example is the development of a self-assessment tool and the request that all systems be associated with a security plan, accredited and certified. Several responding countries report that the formulation of their government policy on security of information systems and networks takes place in a centralised manner.

The security life cycle principles "risk assessment", "security design", "security management" and "reassessment" are implicitly or explicitly reflected in the security management of government systems and networks most frequently through the issuance of guidance by a national agency, national policy or legislation. One country reports the requirement that the implementation of these principles be compliant with an international standard (ISO/IEC 17799/BS7799) and another one mentions a possible reference to international standards in its future policy on the security of information systems and networks.

As regards the security of government systems and networks:

- All respondents have adopted a policy on security management for their government's own systems and networks, or are in the process of doing so (Belgium, Mexico, Portugal).
- The security policy is expressed through recommendations (France, Finland), standards (Denmark), manuals (Australia, Austria, Germany), guidelines (Japan, Korea), or national security policy documents such as the US "National Strategy to Secure Cyberspace".

The United States has developed a self-assessment tool that all agencies are required to use and requires all government's systems to be associated with one security plan, accredited and certified before being made fully operational.

Belgium is working on a national policy for the security of governments systems and networks which would be based on the ISO 17799:2002 standard. The operational implementation of the policy will be based on Information Technology Infrastructure Library (ITIL) management processes. [7]

National policies for the security of government information systems and networks are, or will soon be, formulated in a centralised manner for all respondents except Italy, Norway and the Slovak Republic. These policies are formulated via the publication of a national policy document approved either by the government or the parliament and/or the issuance of guidelines, recommendations, standards or manuals for government administration. Some of these countries stress that the implementation of the policy is decentralised (Belgium, Canada, Czech Republic, Denmark, France, Hungary, Japan, Korea, Netherlands, Norway, Sweden). Three countries report that their government security policy has been developed in a decentralised manner. Norway stressed that agencies which own and operate common infrastructures have established common security policies for all user entities (*e.g.* a central network and services for the ministries or a common network for regional government).

Australia has developed an "Information Security Group" to provide material and assistance to government departments on matters relevant to the security and integrity of official information.

Security Guidelines principles “Risk assessment”, “Security design and implementation”, “Security management” and “Reassessment” are implicitly or explicitly reflected in the security management of government systems and networks through various means, including:

- Guidance, recommendations, tools, or manuals issued by national agencies: Austria, Australia, Finland, France, Germany, Hungary, Spain, United States.
- Specific bodies supporting agencies on the security of information systems and networks (IT Incident Center, Emergency Management Agency): Sweden.
- National policy document: Japan, Netherlands.
- National legislation: Finland, Korea.
- Required compliance with ISO/IEC 17799/BS7799: United Kingdom.

The Belgian policy on security of information systems and networks currently under discussion will be aligned with the above-mentioned principles. Italy is studying the issue of reflecting these principles. Denmark’s “IT Security Plan” does not include these principles, but they will be reflected at implementation stage.

Governments’ influence on other participants (Q17, Q18)

Responding countries have provided very different answers to how they lead by example or develop best practices and other operational improvements for the benefit of all participants. The majority of countries publish guidance. Several countries underline the sharing of information among government bodies and the requirement of specific actions. Others mention some form of co-operation and information sharing with stakeholders.

Most respondents use government purchasing power to influence other participants. A majority of responding countries report required or recommended conformity to standards or guidance for IT procurement. Two countries have a specific body to manage government purchases or assist agencies in choosing products.

To become a “model owner” and lead by example, and to develop best practices and other operational improvements for the benefit of all participants, respondents:

- Write and/or publish guidance, recommendations, manuals, best practices: Australia, Austria, Denmark, Finland, Germany, Hungary, Japan, Netherlands, United Kingdom.
- Share information among government bodies and/or require specific action from government employees and bodies. This includes:
  - Establishing working groups at various levels: Czech Republic, Denmark, Korea, Netherlands.
  - Establishing an Information Management Strategy Committee promoting close collaboration between agencies and requiring government agencies to devise policy to ensure that their information systems are protected: Australia.
  - Constantly updating government’s users and sharing among ministries: Italy.
  - Requiring specific measures such as vulnerability analysis and assessment every year or designation of an information security manager in each ministry: Korea.

- Co-operate and share information with business and relevant communities. For example:
  - Exchanging best practices during multi-organisational projects and publishing the results: Finland.
  - Complying with legislation: Mexico (Transparency and Access of Government's Information).
  - Sharing with relevant communities experience gained from projects (when possible): Norway.
  - Developing best practice concepts through partnerships and promulgating these concepts to assist suppliers and users in interacting with government: United Kingdom.
  - Staying in contact with industry regarding developing best practices and renewing government's own procedures: United States.
- Implement an e-government project (Denmark) and develop and promote secure access to e-government services (Belgium).
- Have specific bodies to give advice and publish reports to support other agencies on the security of information systems and networks (Sweden) or to co-ordinate action regarding e-government and the digital economy within the government administration (France).
- Promote the use of ISO/IEC 15408 certified or recommended products within government: France, Japan. The Swedish Emergency Management Agency plans a study on the use of Common Criteria as a model for security specifications in procurement of security products. Belgium will integrate best practices into ITIL models and standards on operational IT security management.

In order to influence other participants with their purchasing power, respondents mentioned the:

- Required or recommended conformity of IT purchases with international standards such as ISO/IEC 15408/Common Criteria (Japan, Spain, United Kingdom) or ITSEC[8] (United Kingdom), national standards (Czech Republic, Korea[9], United States), or guidance (Finland).
- Required or recommended purchase of certified products: Australia, Germany.
- Designation of a specific body to deal with government purchases and a body to help agencies with product selection: Australia, United Kingdom.
- Use of common contract rules or requirements for IT procurement: Austria, Finland, Hungary.
- Drafting and publishing of a common documentation promoted by the government which some agencies are required to use: France.
- Recommendation to have the budget ratio for the security of information systems and networks reflected in guidelines for budget make-up: Korea.
- Establishment of a PKI infrastructure by the government for secure internal communication and communications with third parties: Netherlands.
- Require the use of digital signatures for online submissions for calls for tender: Belgium.
- Co-ordination of public procurement and development of common purchasing requirements: Portugal.

Denmark, Korea and Norway do not use their purchasing power to directly encourage the development of more secure products. Italy is studying the issue.

D. Government as user of information systems and networks (Q19, Q20)

The majority of responding countries ensure that their use of information systems and networks is consistent with the Security Guidelines. Several countries have a national body that follows and/or checks the implementation of the IT security policy. Except one country which reports the requirement of an annual independent audit for all agencies, no detail was provided on the means used to ensure that government use of information systems and networks is consistent with national policies and the Security Guidelines.

The majority of responding countries have implemented training programmes and tools to increase their employees' awareness of security concerns, of their individual responsibilities, and of their capability to respond to security incidents in an appropriate way. One country mentioned that training for new employees is mandatory through legislation. The use of e-learning tools for the training of local government officials is worth mentioning as well as a self-assessment tool provided by another government.

Responding countries ensure that their use of information systems and networks is consistent with the Security Guidelines by:

- Basing their national policy on security of information systems and networks on the Security Guidelines (Czech Republic, Denmark, Finland, Hungary, Italy, Netherlands) and/or having government security guidance consistent with the Security Guidelines (Australia, United Kingdom), or requiring each ministry/agency to work in line with the Security Guidelines (Japan).
- Having a national agency/body to:
  - Follow the development of IT security in the public and private sectors: Denmark.
  - Check the consistency of government's systems with data protection legislation: France.
  - Co-ordinate and advise authorities, share best practices, produce trend analysis reports, represent the government in national and international standardisation bodies and implement secure networks within the government: Germany.
  - Supervise the implementation of the national policy: Hungary, Netherlands.
  - Ensure that security of information systems and networks is implemented in government systems and networks and inform the users of their security responsibilities: United Kingdom.
- Requiring an annual independent audit for all agencies: United States.
- Development of an E-Government Quality Mark: Austria.
- Developing a framework for the functional organisation of the security of information systems and networks which distinguishes three levels (policy and planning, security control, audit): Belgium.

Norway has not co-ordinated its efforts for active use of the Security Guidelines, as yet.

The majority of respondents have implemented security training programmes and tools for their employees. Belgium is developing such programmes. One country reports that such training is made mandatory for new employees by legislation (United States).

Training programmes are either organised by each ministry/agency (Austria, Czech Republic, Germany, United Kingdom, Netherlands, Norway) with the help of a national agency for the security of information systems and networks (France) or are under the responsibility of a single department (Australia).

They can also be carried out through co-operational, multi-operational projects on security of information systems and networks (Finland).

In some cases, training programmes target IT security officers (United Kingdom), specific populations with given skill levels and organisational needs (United States) or officials of local governments (Japan). In the latter case, the training programme uses e-learning tools, has been followed by 7 000 individuals and will be extended to all government officials.

II. Roles of business and civil society

A. Business as owner, operator and/or user of information systems and networks (Q21, Q22)

Dialogue between government and business to encourage business to address the principles of the Security Guidelines takes place for the majority of responding countries through different means such as workshops, discussion for legislation in preparation and support for ISO/IEC 17799 or public/private partnership. Self-regulatory organisations were mentioned by two respondents.

Most respondents report specific programmes to help business take responsibility for ensuring that their use of information systems and networks is consistent with the Security Guidelines. Examples include promotion of international standards, creation of a trust mark for Internet access or government participation in an association to provide advice to business and help prepare employee training in line with the Security Guidelines.

Government-business dialogue takes place through:

- Events such as seminars and workshops: Finland, Hungary, United States.
- Discussion to prepare legislation: France, Korea.
- Establishment of a “Business-Government Task Force on Critical Infrastructure”: Australia.
- Creation of public/private partnerships: Hungary, Netherlands.
- Promotion of ISO/IEC 17799 (Australia) and support for its Users’ Group Secretariat (United Kingdom).
- Participation in business-government co-operation arenas and endorsement of awareness initiatives taken by business associations: Norway.
- Development and implementation of an E-Government initiative: Austria.

Mexico is making efforts to establish this kind of dialogue between business and government.

Hungary invites representatives from business and civil society for consultation on a case by case basis to the IT security subcommittee of its Inter-Departmental Coordination Committee for the Information Society (IDCCIS).

As regards self-regulatory efforts, the United Kingdom mentioned the tScheme, an industry-led, self-regulatory scheme set up to create strict assessment criteria against which the tScheme organisation will approve trust services. The United States also mentioned business alliances such as the Global Business Dialogue on Electronic Commerce (GBDe) and Transatlantic Business Dialogue (TABD) which have been active in promoting the Security Guidelines through links, frameworks and recommendations.

Eight respondents have specific programmes to help business take responsibility for ensuring that their use of information systems and networks is consistent with the Security Guidelines. These programmes include:

- Promotion of international ISO/IEC standards: Australia, Japan.
- A poll on security risks for SMEs: France.
- Legislation in preparation to promote security training, periodical security checks, assessments, and use of security products in business: Korea.
- Creation of a trust mark for Internet access: Japan.
- Financing studies on the security of information systems and networks in national enterprises according to ISO/IEC 17799: Spain.
- Participation in an association that brings business and government representatives together to provide advice to business in line with the Security Guidelines, and prepare training for employees: Norway.
- Future provision of business guidelines on the security of information systems and networks: Korea.
- Creation of a Web site for business, through a public-private partnership: United Kingdom.

Austria has not yet implemented a programme but is planning for such activities in 2004.

B. Civil society as users of information systems and networks (Q23, Q24)

The majority of responding countries dialogue with civil society to encourage civil society to address the principles of the Security Guidelines. Most initiatives aim at awareness-raising such as the organisation of a national consumer protection week on the theme “Security of Information Systems and Networks”.

The majority of responding governments either dialogue with civil society to address the principles of the Security Guidelines or will do so in the future (Austria, Norway, Mexico, Portugal). The reported means to establish and maintain this dialogue include:

- Publication of information/recommendations on the Web: Australia, Finland, France, Germany, United States.
- Hosting workshops and conferences: France, United States.
- Launch of information campaigns, *e.g.* on how to choose a password: United States.

- Creation of a Committee in which security companies as well as civil groups are participating to discuss developing best practices for the security of information systems and networks and privacy protection: Korea.
- Recommendations from the data protection commissioner: Finland.
- Preferential tax treatment and government loans to encourage SMEs to invest in technologies for the security of information systems and networks: Japan.
- E-government programme offering secure services to citizens and business: United Kingdom.

Belgium, the Czech Republic, Finland, the Slovak Republic and Sweden have no special programmes.

To ensure that individuals' use of information systems and networks is consistent with the Security Guidelines, responding member countries:

- Either have no specific programme (Australia, Austria, Czech Republic, Finland, Korea, Mexico, Norway, Portugal) but mention future activities related to this goal, such as a public/private partnership programme called "National e-Literacy" which provides computer courses to beginners and could include items on the security of information systems and networks in the future (Czech Republic).
- Or refer to awareness-raising initiatives or tools (Germany, Japan, Sweden, United States).

NOTES

1. The OECD Implementation Plan was approved by OECD member countries in 2002 and has been reissued following further revisions as an unclassified document, DSTI/ICCP/REG(2003)5/REV1, for the Oslo OECD Global Forum on Information Systems and Network Security.

2. ISO/IEC 15408 "Evaluation Criteria for Information Technology Security" is also known as "Common Criteria" or "CC".

3. ISO/IEC 17799 is a standard code of practice that provides an organisation with default guidelines on the types of security controls an organisation should implement to safeguard its assets. BS7799 is a management standard specification for Information Security Management Systems (ISMS). This instructs an organisation on the necessary steps required in establishing a management framework.

4. The Safer Internet programme is an EU initiative to fund activities related to the management of undesirable content on the Internet. For more information, see www.europa.eu.int/information_society/programmes/iap/index_en.htm, accessed 14 May 2004.

5. US GetNetWise. See below.

6. A typical CERT provides technical advice and co-ordinates responses to security compromises, identifies trends in intruder activity, works with security experts to identify solutions to security problems, and disseminates information to the broad community. It may also analyse product vulnerabilities, publish technical documents, and present training courses. See www.cert.org. An ISAC is sponsored by a specific industry sector. It is intended to gather, analyse, and disseminate to its members an integrated view of information system and other infrastructure vulnerabilities, threats, and incidents that are relevant to its sponsoring sector. An ISAC may also share best security practices and solutions among its members. See *e.g.* https://www.it-isac.org/, accessed 14 May 2004. SANS is a co-operative research and education organisation. It provides security professionals, auditors, system administrators, and network administrators with resources on security of information systems and networks (news digests, research summaries, security alerts and papers) and training. See www.sans.org.

7. "ITIL provides a cohesive set of best practices, drawn from the public and private sectors internationally. It is supported by a comprehensive qualification scheme, accredited training organisations, and implementation and assessment tools. The best-practice processes promoted in ITIL both support and are supported by the British Standards Institution's Standard for IT Service Management (BS15000)." See www.ogc.gov.uk/index.asp?id=2261, accessed 14 May 2004.

8. Information Technology Security Evaluation Criteria (ITSEC) is recognised throughout Europe. It represents a single uniform standard adopted by France, Germany, Netherlands, United Kingdom and the European Commission, thereby reducing the need for products to be evaluated in individual countries. CC is an ISO standard (ISO15408) and is recognised more widely than ITSEC. See www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=1, accessed 14 May 2004.

9. Security Products, such as firewalls, IDS and VPN need certification by the Korean National Intelligence Service (NIS) to be applied in the public administration. In the future it is envisaged to use the CC instead of national Korean standards.

ANNEX A: LIST OF SURVEY QUESTIONS

I. Roles of government

Q1. Does your government make the Guidelines publicly available? If so, by which means? Hardcopies. Electronically. Link to the OECD Web site. Other (please describe).

Q2. Are the Guidelines translated into your native language(s)? If so, please list the language(s).

Q3. If the Guidelines are available in your native language(s), are they, and related information, available on the Web?

Q4. Does your government recognise and use the Guidelines as a policy framework for information security?

A. Government responsibility for public policy

Q5. Has your government developed a national policy on information security? If yes, please describe.

Q6. Has your government enacted a comprehensive set of substantive criminal, procedural and mutual assistance measures to combat cybercrime and ensure cross-border co-operation […]

Q7. Are these measures as comprehensive as, and consistent with, the Council of Europe Convention on Cybercrime?

B. Outreach and support for other participants

Q8. What kind of programmes and initiatives has your government developed to raise awareness and facilitate responses from all participants who use or are involved with information systems and networks?

Q9. Does your government have a programme to foster the development of best practices, and/or partnerships among participants to address information security?

Q10. Does your government support the exchange of best practices to facilitate users' abilities to better understand and achieve effective and up-to-date security measures?

Q11. Does your government support education and information programmes on information security? For example, does your government have awareness-raising programmes that would include educational programmes, training, Web sites, public announcements and the like that offer tools/kits for promoting a culture of security? If yes, how do they integrate the values of each of the Security Guidelines principles, notably on ethics and democracy?

Q12. Does your government encourage the establishment and utilisation of useful sites (such as those of CERT or SANS and various industry information-sharing and analysis centres (ISAC))? If yes, what kind of initiatives does your government encourage or support?

Q13. Does your government support research and development to increase security through improved security in software, hardware, and best practice operational procedures?

C. Government as owner and operator of information systems and networks

Q14. As owner and operator of information systems and networks, has your government developed a policy on security management of its own systems and networks?

Q15. How does your government formulate its national policy for security of government information systems and networks? Is it centralized or decentralized among individual Ministries?

Q16. How does your government's security management of government systems and networks reflect the Guidelines' principles, notably those related to "risk assessment", "security design", "security management" and "reassessment"?

Q17. How does your government use its systems and networks to become a model owner and to lead by example? How does your government develop best practices and other operational improvements for the benefit of all participants?

Q18. Does your government use its purchasing power in information systems and networks to encourage the development and expanded availability of more secure products and services? If yes, how? Does your government have security guidelines and/or standards that must be followed for procurement of information systems and networks?

D. Government as user of information systems and networks

Q19. As a user of information systems and networks, how does your government ensure that its use is consistent with the Guidelines?

Q20. Has your government developed any programme to enhance the security environment, training and tools to ensure its employees are aware of security concerns, their individual responsibilities, and have the capability to respond in an appropriate way to security incidents?

II. Roles of business and civil society

A. Business as owner, operator and/or user of information systems and networks

Q21. Does your government dialogue with business to encourage business to address the principles of the OECD Security Guidelines? In particular, do they encourage business to take self-regulatory initiatives and to be active independently or in partnership with government and/or civil society to promote best practices, education, and responsible product and service development in line with the guidance of the principles of the Security Guidelines? If yes, please describe.

Q22. Does your government have any programme/activity to help business take responsibility for ensuring that their use of information systems and networks is consistent with the Guidelines?

B. Civil society as users of information systems and networks

Q23. Does your government dialogue with civil society to encourage civil society to address the principles of the OECD Security Guidelines? In particular, do they encourage civil society to be active independently or in partnership with business and/or government to promote best practices, education, and responsible product and service development in line with the guidance of the principles of the Security Guidelines? If yes, please describe.

Q24. Does your government have any programme/activity to help civil society take responsibility for ensuring that individuals' use of information systems and networks is consistent with the Guidelines?