OECD publishing

Please cite this paper as:

OECD (2005-02-16), "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries", *OECD Digital Economy Papers*, No. 102, OECD Publishing, Paris.
http://dx.doi.org/10.1787/232017148827

OECD Digital Economy Papers No. 102

The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries

OECD

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

16-Dec-2005

English - Or. English

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

DSTI/ICCP/REG(2005)1/FINAL
Unclassified

Working Party on Information Security and Privacy

THE PROMOTION OF A CULTURE OF SECURITY FOR INFORMATION SYSTEMS AND NETWORKS IN OECD COUNTRIES

JT00196105

English - Or. English

FOREWORD

This report includes a detailed inventory of effective national initiatives to implement the 2002 OECD "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security". It was prepared by the Secretariat based on responses from 18 OECD member countries to a survey questionnaire circulated in November 2004. The analysis, synthesis and summary of responses contained in the report are current as of September 2005, and are all to be read as an *interpretation* of the information provided. The report follows up on a previous report released in 2003[1] to which all respondents had already contributed.

At its 18th meeting on 19-20 May 2005 in Paris, the Working Party on Information Security and Privacy (WPISP) discussed a first draft of the report and agreed to finalise it by written procedure. The Committee for Information, Computer and Communications Policy (ICCP) discussed the report at its 49th meeting on 6-7 October 2005 and declassified it by written procedure in November 2005.

The report is published under the responsibility of the Secretary-General of the OECD.

1. DSTI/ICCP/REG(2003)8/FINAL; www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp-reg(2003)8-final

EXECUTIVE SUMMARY

This report is a major information resource on governments' effective efforts to date (September 2005) to foster a shift in culture as called for in the 2002 *OECD Guidelines for the Security of Information Systems and Networks*: Towards a Culture of Security. It includes a detailed inventory of initiatives to implement the Guidelines in the following 18 OECD member countries: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Japan, Korea, Netherlands, Norway, Portugal, Slovak Republic, Spain, Sweden, United Kingdom, and the United States. It also highlights main findings based on an analysis of common current trends in those countries and progress made since 2003.

The report is intended to:

- Foster the sharing and dissemination of practical information and best practices among OECD member countries and with non-member economies.
- Help monitor progress in national approaches to information security.
- Be a resource for identifying key issues and best practices to further explore and address.
- Provide new online resources to supplement the OECD "culture of security" Web site.[2]

The report is structured in two parts, including: *1)* the main policy messages based on an *analysis* of the responses; and *2)* a *synthesis* of the responses, question per question. More detailed country summaries and the questionnaire are to be found in Annexes 1 and 2.

Main findings

A first main finding is that *e-government* and the *protection of national critical information infrastructures* appear to be two main drivers for developing a culture of security at the national level.

A second finding is the importance of *international co-operation* for fostering a culture of security and, in particular, the role of regional fora in facilitating interactions and exchanges. International co-operation is consolidated in the area of *cybercrime and Computer Emergency Response Teams* (CERTs).

The report also highlights that member countries are adopting a *multidisciplinary and multi-stakeholder approach* and establishing *a high-level governance structure for the implementation of national policies.* They have made significant progress in both the *development of a national policy framework* and the implementation of the *Awareness and Response Principles*. Almost all countries have adapted their legal frameworks for combating *cybercrime*. All except two countries report one or more *Computer Emergency Response Teams* (CERTs) or *Computer Security Incident Response Teams* (CSIRTs), or are in the process of setting up such a function. *Awareness raising* and *education initiatives* still receive a high degree of attention. The *sharing of best practices*, *development of partnerships among participants*, and *use of international standards* are increasingly taken into consideration.

2. Cf. www.oecd.org/sti/cultureofsecurity

The report shows that responding countries seem to have devoted less attention to developing research and development for information security, metrics and benchmarks for measuring the effectiveness of their national policies, and initiatives for co-ordinated frameworks to address the specific needs of small and medium-sized enterprises (SMEs).

Structure of the synthesis

Part II of the report presents the *main characteristics of national policies and strategies* for the security of information systems and networks in the responding countries. It depicts *national legal, regulatory, and institutional arrangements*, highlighting specific areas such as cybercrime, computer incident watch and warning/response, critical infrastructure, risk assessment, government's outreach to business, civil society, State and local government, education and training, science and technology, research and development, and international co-operation.

The synthesis also includes initiatives for voluntary, publicly available r*ecommendations*, and focuses on actions taken by *governments* as *owners and operators* of systems and networks to develop a culture of security. The most effective information security *programmes and initiatives for users of government systems* are also highlighted, as well as successful governmental initiatives with regard to co-*operation with and outreach to business*, in particular small and medium-sized enterprises (SMEs), and *civil society*. Finally, government efforts related to *science and technology, research and development,* and initiatives for *measuring the impact* and/or success of government initiatives are described.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

Main findings 3
Structure of the synthesis 4

PART I: MAIN FINDINGS 6

1. Key drivers for a culture of security 6
2. Commonalities in approaches to developing and implementing national policies for a culture of security 7
3. International co-operation 8
4. Status of activities 8

PART II: SYNTHESIS OF THE RESPONSES 11

Section 1: Government as developer of public policy, law, and regulation 11
Section II: Government as owner and operator of systems and networks 17
Section III: Government as user of information systems 19
Section IV: Government as partner with business and industry 20
Section V: Government as partner with civil society 23
Section VI: Government efforts related to S&T and R&D 24
Section VII: Metrics and benchmarks 25

ANNEX 1 COUNTRY SUMMARIES 26

I. Government as developer of public policy, law, and regulation 26
II. Government as owner and operator of systems and networks 84
III. Government as user of information systems 91
IV. Government as partner with business and industry 93
V. Government as partner with civil society 115
VI. Government efforts related to S&T and R&D 122
VII. Metrics and benchmarks 125

127

ANNEX 2 OECD QUESTIONNAIRE ON PRACTICAL INITIATIVES TO PROMOTE A CULTURE OF SECURITY AS CALLED FOR IN THE OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: TOWARDS A CULTURE OF SECURITY 128

Section I: Government as developer of public policy, law, and regulation 128
A. Comprehensive statement of strategy 128
B. Legal, regulatory, and institutional arrangements to oversee and implement a culture of security 129
C. Recommendations and other voluntary efforts 129
Section II: Government as owner and operator of systems and networks 130
Section III: Government as user of information systems 131
Section IV: Government as partner with business and industry 131
Section V: Government as partner with civil society 132
Section VI: Government efforts related to S&T and R&D 132
Section VII: Metrics and benchmarks 133

PART I: MAIN FINDINGS

This chapter offers an analysis of the survey findings broken into a few main themes. It includes the main policy messages derived from member countries' responses. As many references as possible are made to the results of the 2003 survey.[3] When interpreting the information contained in the report, and especially when comparing results from the 2003 and 2005 surveys, it needs to be kept in mind that the 2005 survey asked respondents to provide information about their *most successful activities* in an area, and not all activities in each area.

1. Key drivers for a culture of security

The survey has identified two main drivers which support the development of a culture of security at the national level:

- E-government applications and services.
- Protection of national critical information infrastructures.

E-government applications and services

As indicated in most responses, national administrations are implementing e-government applications and services to both improve their internal operations and provide better services to the private sector and to citizens. These initiatives have a common policy characteristic: they do not address the security of information systems and network solely from the technological perspective. They encompass elements such as risk prevention, risk management and users' awareness. Public officials are increasingly aware of the importance of information security for the overall success of government online activities.

Interestingly, by comparison with the 2003 survey, the beneficial impact of e-government activities is moving beyond the public administration towards the private sector and individuals. E-government initiatives appear to act as a multiplier fostering the diffusion of a culture of security. For example, two countries request the private sector and citizens to implement information security controls and approaches within their own information and network systems as a prerequisite to securely accessing government services or to exchanging data with public administrations. As a result, companies and citizens are provided with guidance, best practices and documentation about information security. They are also invited to participate in events such as conferences and workshops where they are made aware of issues associated with information and network security.

The protection of national critical information infrastructures

The survey also shows that the protection of critical information infrastructures is another core area for the development and implementation of national policies for the security of information systems and networks. Government, industry, citizens and society at large rely on a number of critical information infrastructures (*e.g.* energy, water supply, transport, financial sector, telecommunications, health-care services), and the need to avoid any disruption in the operation of these infrastructures has led governments to develop and implement policies aimed at reaching out to industry, as the primary owner and operator of these infrastructures. In some countries, the dialogue between industry and government has been facilitated through the establishment of public-private partnerships and the sharing of best practices and information about the technical, management and human complexities of information systems and networks security.

3. DSTI/ICCP/REG(2003)8/FINAL; www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp-reg(2003)8-final

Privacy as an indirect driver

Several responses also indicate that national privacy legislation is an additional indirect driver for the development of a culture of security. In particular, the need to protect personal data, *inter alia*, is important for the success of e-government activities targeting citizens, and has led both public and private organisations to consider information security as a means to satisfy privacy requirements. In several countries, security awareness-raising activities have been organised to help organisations satisfy privacy needs and legal requirements. These initiatives seem to have acted as a multiplier for the development of both security and privacy policies.

2. Commonalities in approaches to developing and implementing national policies for a culture of security

Almost all countries have finalised their national strategy for fostering a culture of security.

Interestingly, the survey highlights two main commonalities in member countries' approach to developing and implementing national policies for a culture of security. Governments adopt:

- A multidisciplinary and multi-stakeholder approach.
- A high-level governance structure.

Multidisciplinary and multi-stakeholder approach

National policies for the security of information systems and networks share a common characteristic: they are the result of a multidisciplinary and multi-stakeholder approach. Responses emphasise that a culture of information security cannot just arise from technical solutions. A comprehensive approach is needed that addresses socio-economic and legal considerations, hence the multidisciplinary dimension of national policies. Further, governments alone cannot address the whole range of issues associated with fostering a culture of security, hence the involvement of the private sector and civil society. However, differences appear in the way this multi-stakeholder approach is implemented. As illustrated in three countries, the private sector and civil society can be directly involved through public-private partnerships, the development of best practices and other common initiatives. In other countries, they provide advice and overall policy support by taking part in working groups or advisory councils.

Responses also show that governments frequently resort to industry for advice on technological developments and overall implementation issues. As indicated by two countries, they may contract with academics and independent experts who are tasked with providing policy advice and/or evidence to justify the need to develop certain policies. Finally, the survey indicates the limited direct involvement of civil society representatives in preparing national or sector-based information security policies. Their role is foreseen, instead, in the implementation phase.

High-level governance structure

Responses confirm the findings of the 2003 survey with respect to national governance structures for the implementation of a culture of security. National policies for the security of information systems and networks are, in most cases, endorsed at the highest government level. National policy implementation is almost equally delegated to either an organisation set within the prime minister's or executive office or to a government department and ministry. In two countries, however, the responsibility for implementing the information security policy is split between two or three ministries.

3. International co-operation

The survey indicates that responding countries appreciate the importance of international co-operation for fostering a culture of security, and have undertaken to pursue such co-operation in specific areas. A majority of respondents are actively involved in international networks and other co-operation activities for combating cybercrime. A similar situation emerges in the area of CERTs. Several have established operational networks through which they exchange information and best practices. One country is also supporting the development of CERTs in other economies as well as the involvement of these CERTs at the regional level. One country reports the establishment of a regional advisory body aimed at fostering common policies and approaches for electronic signatures both at national and international levels.

It seems that in most other areas, international co-operation is limited to the sharing of best practices and guidance, for example through conferences and workshops, and that interactions and exchanges between countries are undertaken primarily through regional fora.

4. Status of activities

In 2003, the survey showed that member countries had placed the highest degree of attention on the development or amendment of a national policy framework and on the implementation of the Awareness and Response Principles. Responses in 2005 indicate that important progress has been made in these areas and, further, that initiatives to combat cybercrime have been consolidated.

In 2003, the survey also highlighted that a lower degree of attention had been placed on issues such as the sharing of best practices, the development of partnerships among participants, and the use of international standards. In 2005, while there is still room for improvement, these issues are receiving more attention. However, three important areas emerge that still appear to receive a more limited degree of attention: research and development, evaluation and assessment measures, and outreach to SMEs.

Areas of high attention

Responding countries have primarily directed their efforts to:

- Combating cybercrime.
- Developing Computer Emergency Response Teams (CERTs).
- Raising awareness.
- Fostering education.

Cybercrime

Almost all countries have adapted their legal frameworks to tackle cybercrime issues. Many indicate the Council of Europe's Convention on Cybercrime and relevant European Union legislative acts as the main reference documents. Moreover, respondents indicate that they have established a central function or co-ordinating body to tackle different forms of cybercrime. These bodies are also co-operating with the private sector and engaging in international co-operation efforts to better respond to the global nature of cybercrime. Finally, some countries report that their "cybercrime" unit is also engaged in awareness activities for the private sector, in particular SMEs, and for citizens.

Computer Emergency Response Teams (CERTs)

Today, all responding countries report having a national CERT or CSIRT (Computer Security Incident Response Teams), or are in the process of setting up such a function. In some countries, there are also CERTs specifically tasked to address the needs of public organisations or private institutions. In two countries, the activities of CERTs are paralleled by Information Sharing and Advisory Centres (ISACs).

These bodies facilitate the sharing of security information within a group of members operating in similar commercial sectors. International co-operation, finally, is considered an integral and important part of the activities of national CERTs, since it allows a broader exchange of information and best practices.

Awareness raising activities

As already shown by the 2003 survey, respondents are actively taking initiatives to raise awareness of the need for a culture of security. These initiatives involve both the organisation of public events and the distribution of informative material. Issues addressed in public events vary from general information security issues to more specific ones like risk management, electronic authentication, electronic signatures and PKI. The target groups for awareness-raising vary from the general public to experts working in public and private organisations. In particular, governments continue to foster a culture of security among public officials through a large variety of seminars, workshops and conferences. Interestingly, in two countries, national administrations have extended participation in such events to the private sector and citizens. This approach illustrates how government initiatives can impact the private sector and the citizens.

As in 2003, the preparation and distribution of free recommendations, best practices and guidance are seen as important vehicles for fostering a culture of security. However, several countries seem to focus increasingly on drafting best practices on specific technical and operational topics like online authentication, digital signatures, wireless, peer-to-peer networking, risk management and incident response. Finally, two countries are experimenting innovative dissemination channels like SMS, text TV and instant messaging.

Education

Many respondents report interesting initiatives in this domain. Institutions tasked with education initiatives range from government agencies specialising in IT security to law enforcement agencies dealing with cybercrime. As for raising awareness, education initiatives involve the free distribution of education material. In one country, these education activities are conducted using Internet-based delivery channels like a forum specifically dedicated to the security of information and network systems. Some countries have also reported measures targeting school teachers who act as multipliers by passing on information security knowledge to students. The private sector is sometimes involved in these activities. This is the case in one country where industry provided its perspective on best practices for information security education and training purposes. In this country, a task force established by a public-private partnership has made suggestions on how public/private national outreach campaigns could reach a large part of the population and SMEs within one year using a combination of advertisements in the popular press, and through partnering with Internet Service Providers (ISP) and providers of security solutions.

Areas of lower attention

The few areas on which responding countries have not yet placed a high degree of attention include in particular the following:

- Research and Development.
- Evaluation and Assessment.
- Outreach to SMEs.

Research and development

As already indicated in the 2003 survey, responding countries recognise the importance of research and development (R&D) activities for fostering the security of information and network systems. R&D is key to developing innovative solutions to tackle present and future complex information security

requirements. Investments in R&D for information security are also seen as contributing to raising the overall level of innovation and competitiveness. Nevertheless, only four countries have established publicly-funded programmes aimed to support research specifically focused on information security. All other respondents indicate that R&D activities related to information security are undertaken as part of more widely defined research programmes. Furthermore, R&D for information security continues to be mainly focused on computational and technological aspects while one country indicates taking the social and economic dimensions of information security into consideration.

The survey also indicates that research activities are conducted within universities, sometimes by institutes dedicated to R&D in information security and, with less frequency, in co-operation with industry. Finally, with the exception of three countries, the survey also shows a limited focus on international co-operation for R&D.

Evaluation and assessment

The survey indicates that, with one exception, responding countries do not have specific metrics and benchmarks to assess the overall effectiveness of their national policy to develop a culture of security. Two countries have started to develop specific evaluation tools and instruments, while the others use the standard evaluation methodologies applicable to all national policy initiatives.[4]

Several countries have established methodologies and procedures to assess the level of security of their government information systems and networks. They conduct security assessments on the basis of national standards. However, these most often do not directly refer to international standards, thus limiting any comparative analysis across countries.

Finally a few countries have provided data about their national public spending on information systems and network, but the heterogeneous nature of their current data does not allow for a comparison.

Outreach to SMEs

Responses to the 2003 survey indicated that some member countries have already taken initiatives specifically targeting SMEs. Their focus was primarily in the area of awareness raising and, to a lesser extent, alert and response. In 2005 almost all respondents had undertaken specific efforts towards SMEs. In some cases, these efforts have gone beyond awareness-raising to include, for example, the provision of technical information and some form of financial support. However, only three countries have initiated a direct dialogue with organisations representing SMEs. Finally, no country has reported a co-ordinated framework to address the specific information security needs of SMEs.

4. Current work on Indicators for Trust by the OECD Working Party on Indicators for the Information Society (WPIIS) [DSTI/ICCP/IIS(2005)1/FINAL] could be useful in this context.

PART II: SYNTHESIS OF THE RESPONSES

This Chapter provides a synthesis for each question that was asked[5] of member countries' responses, question per question.

Section 1: Government as developer of public policy, law, and regulation[6]

A. Comprehensive statement of strategy

Development of a national policy and/or strategy on the security of information systems and networks and the promotion of a culture of security (Q1)

The development of a national strategy aimed at fostering the security of a country's information infrastructures is a constant among all respondents. These policies call for the need to develop research and development and to enhance public awareness about the increasingly large number of online threats and vulnerabilities. In some cases, national policies have been developed by bringing together and co-ordinating into a single policy pre-existing individual activities completed by initiatives tailored to address specific security issues and concerns. In other cases, national policies have built upon initiatives aimed at developing and implementing e-government policies or specific initiatives such as citizen cards or digital signatures.

National policies promote a multidisciplinary and multi-stakeholder approach indicating that technical applications or responses will not by themselves provide the answers or solutions to tackle information security risks. There is a need for a comprehensive approach that considers human and general management issues. Moreover, a top-down government approach is not sufficient. Close co-operation with industry and all actors involved in the information society with the government as a co-ordinator of these efforts and activities is required. Looking beyond national borders and co-operating with other governments and international institutions is recognised as an important element of any policy since national responses are insufficient to respond to the global information security risks.

The implementation and co-ordination of national policies is usually delegated either to one central body or organisation set within the prime minister's or executive offices or to a government department or ministry. In some cases, this responsibility lies within different ministries due to shared or overlapping policy missions. These bodies or organisations report regularly about their activities and initiatives through traditional means like reports and official documents, as well as Web sites and other online presences.

B. Legal, regulatory, and institutional arrangements

Legal, regulatory and institutional arrangements to implement a culture of security (Q2)

Many respondents report interesting information on their legal framework for authentication, and some, more specifically, on the use of electronic signatures in their country, including provisions for certificate service providers (Austria, Norway and Spain). In Denmark, a legal obligation is made to public entities to offer communication secured through encryption facilities based on the use of digital signatures.

5. Cf. questionnaire in Annex 2.

6. Questions 1 to 3 are primarily related to the policy-oriented principles (1-5) of the 2002 *OECD Security Guidelines.*

Some countries indicate that digital signatures may play an important role for enhancing security in different contexts (for example, e-government, or critical informal infrastructures).

Some respondents also mention their legislation on privacy and the protection of personal data as an overarching component of their legal frameworks for the security of information systems and networks. Relevant provisions comprise obligations for data processors, including providers of services and networks, to secure the personal information stored and processed by their systems and networks, and thus the systems and networks themselves. Legal frameworks are complemented by oversight mechanisms through independent authorities (*e.g.* privacy commissioners) (Austria, Finland, the Netherlands and Norway).

In addition, and more specifically, respondents point out legal frameworks obliging providers of telecommunications services to secure their services and networks. Measures taken are in many cases subject to third-party audits by the respective regulatory authorities, and are enforceable through law and/or through licensing conditions (Austria, Finland, Norway, Spain and Sweden). These regulations are also mentioned as an overarching element, as well as a specific instrument for the protection of critical information infrastructures.

a) Cybercrime

In the area of cybercrime, almost all respondents report that a central function, or co-ordinating body in the law enforcement administration investigates such crimes, with specifically equipped and trained personnel. In many cases the central body is supplemented by corresponding units at the regional and local levels. In some countries, these institutions *inter alia* comprise seconded personnel from government, and from the private sector.

Almost all respondents indicate that their legal framework (penal codes and criminal procedures) is aligned with the emerging new threats and new forms of criminal activity, or is in the process of being aligned. Many cite the Cybercrime Convention of the Council of Europe as a reference document for their activities. Procedures for ratification of the Convention are in process in ten responding countries. Some respondents also make reference to a draft framework decision of the European Union on attacks on information systems as a further point of reference for their national activities. Two countries recalled that many forms of cybercrime were already covered under existing legislation.

Some institutions co-ordinate law enforcement activities in the public administration and also liaise with the private sector (Australia, Japan, (with ISPs) and the United States), in one case at the regional level, in order to better take into account local community needs (United States). Japan reports setting up co-ordination bodies for investigation of and response to cyberterrorism on a case-by-case basis. In some cases, the central or regional specialist units also train police officers at the regional and/or local level. Japan also hires experts from the private sector to train police officers in computer forensics. The United States has set up an Internet Complaints Center to facilitate the reporting of cybercrime.

As regards international co-operation, Austria is active in the framework of the European Network of Forensic Science Institutes on Computer Crime (ENFSI). Other respondents co-operate in the framework of Interpol (Austria), the European Union, the Council of Europe, and the G8 (Germany, United Kingdom), more specifically in the G8 24/7 high tech crime network (Germany, United Kingdom and the United States). Bilateral co-operation on a case-by-case basis is frequent.

b) Computer incident watch and warning, and response

Almost all respondents have a CERT or CSIRT function, or are in the process of setting up such a function (Slovak Republic). Some countries report more than one of these organisations, with specific CERTs serving the needs of different communities (*e.g.* governments[7] or a specific industry sector).

Regional and international co-operation is an integral part of the activities of these bodies. Most countries co-operate at the regional (European TF-CSIRT and EGC, APCERT), or global level (FIRST). One country (Canada) explicitly refers to this co-operation being conducted on a 24 hours a day/7 days a week (24/7) basis. 24/7 information security operations and services are under development in Finland.

In Japan and the United States, ISAC structures for the telecom sector collect and share security information among their members. Austria has taken a similar initiative, which is not sector-specific.

Canada develops a national exercise program involving partners from the public and the private sectors to foster emergency management capacities. The United States has published a Computer Security Incident Handling Guide.

Some countries operate traffic monitoring systems to be informed about emerging threats and vulnerabilities in due time, based on information from local networks provided by major telecom operators and controlling agencies (Japan in the public sector and Korea in the private sector), or are conducting research for setting up such a structure (United States).

c) Critical infrastructure

Activities for the protection of critical information infrastructure include protection or action plans (Japan, Norway and the United States) and strategies (United States) which, for example describe responsibilities, best practices and procedures for responding to different kinds of incidents. Australia and Canada are in the process of developing such items. Some respondents have undertaken extensive studies in preparation of these measures (France, Germany).

Respondents have set up permanent committees (Japan and Korea), working groups (Germany), advisory councils (Australia), a cross-departmental centre (United Kingdom) or projects (Netherlands) to facilitate and foster the sharing of information about critical information infrastructures within the public sector, but also between the public and private sectors. In a few cases, citizens are also reported to be part of those networks (Netherlands and the United States). In one country, the network also serves as an alert system (Norway). These structures operate at the national level, but some respondents have similar measures in place at the regional level and for specific sectors.

Co-operative efforts especially between governments and the private sector are frequent, as a large portion of the infrastructure in question is in most responding countries owned and operated by private entities. The United States reports the share of private sector ownership to be an estimated 85%. Some respondents have established co-ordinating bodies in the public administration, sometimes similar to those in place for information security.

Some countries also have taken legal measures in the context of protecting critical infrastructures, or are in the process of revising their legal framework (France): Spain reports sectoral legislation for the telecommunications sector, the United States has taken legal measures to restrict access of the public to

7. See question 4.

critical infrastructure information communicated to the public administration by private owners and operators on a voluntary basis.

Japan plans to create minimum technical and operational standards to be met by information systems. In Japan, the police plays a role with respect to prevention, through visiting critical infrastructure operators and asking them to improve security measures for their infrastructures. Japan also conducts cyber-exercises for information systems of e-commerce companies, operates an Internet traffic monitoring system and a vulnerability handling framework.

Finland has a public information security instruction for critical ICT systems, issued by the Ministry of Finance.

d) Risk assessment

Eleven respondents (Austria, Canada, Finland, France, Japan, Korea, Norway, Spain, Sweden, the United Kingdom and the United States) report specific initiatives with regard to risk assessment. These include the development of methodologies (France and Spain), and standards and guidelines (Norway, Japan, United States). France has completed its EBIOS methodology with a network of users (EBIOS club) to foster exchange of information, and further develop the methodology. Apart from being conducted for information systems and networks, risk assessment is also reported to be applied in other areas, for example natural disasters (Canada and the Unites States), specific national security-critical events (United States), for the telecommunications sector (United States) or, more broadly, for the protection of critical infrastructures (Canada). In Austria, risk assessment is part of the supervision and accreditation of certification service providers. In Finland, risk assessment has played a major part in several co-operational projects for information security led by the Ministry of Finance. Moreover, the Government Information Security Management Board (VAHTI) has prepared a specific instruction for risk assessment.

e) Outreach to business, civil society and others

The majority of respondents to the survey report interesting activities and initiatives regarding outreach to business, and civil society.

Co-operative efforts in one case include the secondment of personnel from the private sector to a national high tech crime centre (Australia). Austria has founded an association to consolidate and develop know-how on IT security for public authorities, businesses, and civil society.

Partners for outreach by governments are most frequently businesses (Austria, Australia, Canada, France, Japan, Korea, Spain, the United Kingdom and the United States). The United States has set up a variety of public-private partnerships to reach out to business, but also to consumer groups, trade associations, non-profit organisations, and corporations. Canada reports to be a partner in the Security Co-operation Program of a large software company.

Areas of co-operation include the security of information systems and networks, but also, more broadly, the protection of critical infrastructures (Australia and the Netherlands), as well as combating cybercrime (Australia). France uses its information technology certification scheme to reach out to the private sector. Austria has an IT security handbook, which can be used across sectors to establish comprehensive IT security processes.

Other activities include awareness raising (United States, for SMEs), *e.g.* the setting up of Web sites and portals (Japan, Norway, Spain), seminars directed at general IT users, or system administrators (Japan, Norway), “road shows” (Spain), and “culture of security campaigns” and competitions (Korea). France hosts workshops on security of information systems and networks with participants from the public and the

private sectors to validate good practices for a given technical topic (*e.g.* remote access or authentication). In Finland, business, civil society and local authorities are increasingly utilising information security material prepared by the Finnish Government (for example, the instructions of the Government Information Security Management Board VAHTI).

f) Outreach to state and local government

Twelve countries (Austria, Australia, Canada, Finland, France, Germany, Japan, Korea, Spain, Sweden, the United Kingdom and the United States) report examples of how their central government reaches out to state and local government. These include setting up co-ordinating bodies with representatives from the state and/or local level (Australia – cybercrime centre AHTCC, and TISN information sharing network, Austria, Canada), or making guidelines for security available to local government (Austria, Finland, Japan). France prepared a law to oblige local administration to take information security into account and conduct risk assessments when communicating over the Internet. Some countries provide training (the United States on investigation of cybercrime) and information resources (*e.g.* Web portals, tools in France and in Germany) to support public bodies at the local level. Japan is implementing financial arrangements to allow local government agencies to buy equipment required to enhance network security. Austria and Germany, through their e-government activities, make available secure software components for use at the state and local levels. Korea has been offering financial and technical support to local governments to re-enforce the security of their IT systems.

g) Education and training

The majority of respondents report activities with regard to education and training, including specific programs at universities. Since 2003, member countries have enhanced their efforts in this area, especially as regards post-secondary education. In some countries, training is also offered by institutions from the private sector. Some countries have created specific entities in the public sector for security information and training of government employees. The United States have guiding material on general Information Technology Security Training Requirements, and for building an Information Technology Security Awareness and Training Program.

Many respondents make educational material (*e.g.* instructions, and in one case, curricula and model documents for use in schools) available on the Internet (in one case in other languages in addition to the national language). As mentioned above, a number of respondents make specific reference to training activities for investigators in the context of combating cybercrime.

While international co-operation for education and training is less frequent, activities reported by members of both OECD and APEC include cross-border initiatives to help less developed economies. A mock security incident training in three countries was also reported.

h) Science and technology (S&T) and research and development (R&D)

Ten respondents (Austria, Canada, France, Germany, Japan, Korea, Norway, Spain, the United Kingdom and the United States) report initiatives in science and technology (S&T) and research and development (R&D). Most are conducted at universities, sometimes in the framework of security-specific programmes, and also, although less frequent, in co-operation with public and private entities. In some countries, universities have set up specific institutes for R&D in information security. Only a few initiatives involving co-operation across borders between the various actors have been mentioned. Interestingly, almost all report R&D initiatives focus on technological development. With one exception, initiatives in this area do not examine the broader societal or economic implications of information security.

i) International outreach and co-operation

Almost all respondents take initiatives with respect to international outreach and co-operation. These include a range of global, international, regional, and bilateral activities. Some OECD member countries are also active in other regional fora dealing with information security (for example, APEC and ASEM). While many initiatives include only government bodies, there are also examples of cross-border efforts across sectors, including partners from business and academia. Furthermore, one country mentions ongoing activities in the Asian region with respect to cross-border sharing of information, *e.g.* of statistical data about Internet traffic, in the framework of watch and warning initiatives across borders.

C. Recommendations and other voluntary efforts

Development of voluntary, publicly available recommendations to assist government, business and/or users to address the security of information systems and networks (Q3)

Responding countries support the preparation and distribution of free recommendations and guides which play an important role in fostering information security awareness among government institutions, industry and civil society as a whole. These activities are either managed by the same central authority that is responsible for the implementation of the national information security strategy (Australia, Austria, Canada, Denmark, Finland, France, Germany, Japan, Korea, Netherlands, Portugal, Spain, Sweden, United States) and/or by specific organisations such as computer emergency response teams, national standardisation bodies or research institutions (Finland, Netherlands, United States)

The distributed documents come in different formats. They range from small brochures to large and more detailed information packages. The content also varies. They can be handbooks with detailed guidance on how to address technical and management complexities of information security (Australia, Austria, Germany, Finland, France, Korea, Netherlands, Japan, Portugal, Sweden and the United States). In other cases, they describe specific technology and management processes such as online authentication, digital signatures, public key infrastructures, wireless and peer-to-peer communications, risk management and incident responses (Austria, Finland, Netherlands, Portugal, the United States and Finland). Finally, the documents sometimes list general principles to be taken into consideration in developing specific applications or services (Canada, France, Finland and Japan). When appropriate, the principles refer back to the OECD *Security Guidelines*. In this context, an interesting example is the Industry Canada booklet "Principles for Electronic Authentication".

Distribution of these publications and information packages involves a mix of online and offline channels. All responding countries involved in these activities freely post these documents on their institutional Web sites. Some documents are in English in addition to the mother tongue of the country. Some countries (Korea and the United States) have also published articles and announcements in the country's leading newspapers and magazines. Several countries (Korea, Netherlands, Japan, Sweden, the United Kingdom and the United States) also develop online newsletters, or use innovative online distribution channels like instant messaging, SMS or text-TV. As regards the offline channels, most (Canada, Australia, Netherlands and the United States) include seminars, conferences and meetings organised by governments to present the material and raise public awareness, often together with industry associations or public-private organisations. In some cases, synergies are established between public awareness efforts in the information security domain and other important topics like the promotion of e-government (the United States, France, Austria and Germany).

Section II: Government as owner and operator of systems and networks

Actions taken by the government to develop a culture of security within the government itself (Q4)

Thirteen responding countries mention an existing (Australia, Austria, Canada, Finland, France, Japan, Netherlands, Sweden, the United Kingdom and the United States) or forthcoming (Czech Republic, Portugal, Slovak Republic) policy for the security of information systems and networks that develops a culture of security within the public administration. In four countries this policy is specific to the public sector while in three others it applies both to the public and to the private sectors. In most cases, the responsibility for co-ordinating the implementation of the policy falls within the mandate of an agency or a ministry body. In two countries, the agency's mandate encompasses both the public and the private sectors whereas in other countries the agency is responsible only for implementation in the public sector. The activities of the agencies vary from: developing policy and standards, to co-ordinating its implementation, to providing consulting, training, audit and even recruitment services for public bodies.

Five sets of initiatives and measures can be distinguished:

- **Watch and warning and incident response** initiatives (Australia, Canada, France, Germany, Japan, Korea, Netherlands, Norway, Slovak Republic (planned), Sweden, the United Kingdom, and the United States). In most cases, services have been developed to provide agencies with alert information and to allow for reporting incidents. Some CERTs carry out other activities such as workshops and conferences (*e.g.* Netherlands). Japan's response teams work in co-ordination with a 24/7 anti-cyber terrorism police force. The United States brought together practitioners of federal agency emergency response teams in a Forum (GFIRST) to allow for information exchange and better co-ordination. Only two initiatives involving four countries (Australia, France, Germany and the United States) report **international activities**: Australia is leading an initiative to help other countries in the APEC region to develop CERT capability and to create a regional CERT communication network and Germany hosted with the United States the International Watch, Warning and Incident Response (IWWN) workshop in Berlin in 2004 and plans other international projects in 2005. France hosted an IWWN workshop in March 2005.
- **Compliance of the public administration with standards, recommendations or manuals** (Austria, Canada, Denmark, Finland, Germany, Netherlands, Slovak Republic (planned), United Kingdom, United States). Standards derived from or at the origin of ISO 17799 are used by Denmark, the Netherlands and the United Kingdom. Austria, Canada and Germany have developed their own standards or IT security manual. Canada is developing a new security management standard which will provide an overall framework for including IT security risks within a corporate risk profile.[8]
- **Development of a PKI** for communication with and within government's administrations (Austria, Finland, Netherlands, Norway).
- **Software development** by public administrations (Austria and Germany). Examples of applications developed in Austria include e-government applications related to the citizen card, a service to check the compliance of e-mail services with e-mail policy and tools for secure wireless communications. In Germany, examples include the Secure Inter-Network Architecture (SINA) which allows for secure transmission of information on insecure networks and the open-source project "Ägypten" for secure and interoperable e-mail.[9]

8. As regards standards and recommendations, see also question 8.

9. See also this item under question 8.

- **Other** interesting initiatives taken by responding countries include:
  - Making the appointment of an IT security officer in each ministry and the adoption of an IT security policy in each unit mandatory (Austria).
  - Fostering co-ordination, collaboration and information exchanges using a Web forum (Canada) or by organising various working groups and forums such as (United States) the Chief Information Security Officers Forum, the Government Forum of Incident Response and Security Team, the Federal Computer Security Program Manager's Forum and the Information Security and Privacy Advisory Board.
  - Providing penetration tests for public administrations through an IT penetration centre (Germany).
  - Providing consulting, training and advice to public bodies (France, Korea).
  - Developing a secure and reliable communication network for emergency services (police, fire, ambulance, army) (the Netherlands).
  - Establishing a central backup system for information systems operated by the public administration (Austria).
  - Implementing co-operative projects to strengthen the culture of security among government agencies (Finland). The Finnish Ministry of Finance and VAHTI have implemented several inter-governmental information security projects to develop risk assessment, information security policies, information security planning, and for the preparation of instructions in ministries and agencies.

Some countries also mentioned "critical infrastructure protection" initiatives. As an example, in Canada, administrations have the obligation to maintain an inventory of critical systems and services and to complete a business continuity plan for these systems.

Finally, only a few countries mentioned measures to evaluate the efficiency of the policy and of its implementation (Canada, Denmark, Japan, the Netherlands and the United Kingdom). An interesting example is provided by the Canadian government which requires each department to undertake internal audits and annual reviews of IT security based on a self-assessment tool developed by the government. The audits are reported to the federal agency responsible for monitoring the implementation of the policy (Treasury Board Secretariat). A government-wide self-assessment was carried out in 2004. In 2002 and 2005, the Auditor General of Canada conducted a government-wide IT security audit which led to policy recommendations.

Information and/or statistics collected on the budget for security of information systems and networks in the public sector. Targets set for the proportion of information security spending in the public sector[10] *(Q5).*

Fourteen out of eighteen respondents answered this question. Seven (Austria, Czech Republic, Finland, Netherlands, Slovak Republic, Sweden and the United Kingdom) do not collect statistics on the budget for security of information systems and networks in the public sector and do not provide further information. Three countries (Finland, France and the Netherlands) note that information security budgets are incorporated in the IT budgets for individual ministries. Four other countries report collecting budget figures for information security (Canada, Germany, Korea, United States) but only two provide figures:

10. This question was primarily related to the policy-oriented principles (1-5) of the 2002 *OECD Security Guidelines.*

Germany reports an estimation of growth for spending as a percentage (between 2001 and 2004: 100% overall budget increase and 50% budget increase for the Federal Office for Information Security). Korea mentions a survey carried out in 2003 and 2004 which concluded that the ratio of the security budget in the overall IT budget was respectively 2.77% and 3.31%.

France reports the absence of systematic collection of information but provides a budget figure (EUR 180 million) for the State Information System Security Reinforcement Plan 2004-2007. Australia mentions EUR 14.8 million over four years for national infrastructure protection.

The types of figures reported and the absence of a common definition for IT security spending make any comparisons difficult.

No respondent reports setting targets for the share of information security spending in the public sector or has plans to do so in the future. Denmark mentions that research shows that such a target should be 10% of the IT budget. The Canadian Treasury Board Secretariat will establish target levels of investment in common security infrastructure and services to improve government-wide efficiency.

Section III: Government as user of information systems

Most effective programmes and initiatives to develop a culture of security among users of government systems (Q6) [11]

Most responding countries have undertaken several specific initiatives to foster the overall security of government information systems by directly engaging public sector administrators about risks and vulnerabilities. A major push for these activities originates from e-government programmes and implementations among central and local public authorities. Interesting examples include, in Austria, the development of the citizen card which has rapidly fostered a strong culture of security among federal and regional public sector officials. This card, in fact, provides Austrian individuals and legal persons with an electronic signature and other technical means to securely interact with the public administration. Likewise, France's EBIOS risk management approach has played a significant role in fostering risk assessment skills and approaches within government ministries and administrative offices. The use of smart cards and PKI for e-mail between different ministries and agencies has strengthened the culture of security of participants in Finland, where the use of framework contracts for information security products has also made it easier and faster for ministries and agencies to start using specific information security products.

The responses indicate that the success of these initiatives is not just related to the quality of the content of the documents produced but also to their dissemination through seminars and/or conferences. In particular, in Japan, the National Incident Response Team organised seminars tailored for public officials in charge of co-ordinating emergency responses. Similar activities are also undertaken by Korea's IT official training centre. Often, these activities do not only target government officials. They are open to the private sector, as in the case of Canada, where the government has launched an initiative to assist SMEs in addressing security and privacy requirements.

11. Question 6 is primarily related to the operation-oriented principles (6-9) of the 2002 *OECD Security Guidelines.*

Section IV: Government as partner with business and industry

Most successful government collaborative initiatives with, and outreach to, small and medium-sized enterprises (SMEs) to promote a culture of security (Q7).

Almost all respondents report initiatives directed at small and medium-sized enterprises (SME). In three countries, an ongoing dialogue with business associations helped design and/or implement the initiatives (Canada, Denmark, Germany) and two countries (Germany and the United States) mention the use of public-private partnerships. Several countries report initiatives targeting home users and micro or small enterprises at the same time (Japan, Netherlands, Spain, Sweden and the United States). Technical information provided to SMEs is delivered in an understandable non-technical language, or in both non-technical and technical languages. The United States reports plans for assessing the effectiveness of its various approaches and material.

Portugal plans to include SMEs in the National Information Security Framework and outlined its strategy to create national awareness about information security. Two countries (Czech Republic and Slovak republic) reported no initiative.

Initiatives include:

- Making information material available (off line and on line), *e.g.* booklets, manuals, handbooks, model policies and concepts, and SME-specific protection profiles: Australia, Austria, Canada, Germany, Sweden, United Kingdom, United States.
- Setting up Web sites specifically targeted at SMEs: Canada, Germany, Japan and Sweden.
- Providing an alert system on emerging threats specifically tailored to the needs of users with little or no technical knowledge: Germany,[12] Netherlands, United States.
- Provision of (online) training (*e.g.* for system administrators, or users): Korea, United States.
- Seminars, conferences and workshops: Austria, Canada, Finland.
- Setting up a specific unit in a government agency to provide technical advice and assistance to IT security product manufacturers so as to increase the security of their products in the design phase, and to facilitate the certification process: France.
- Conducting online and on-site security check-ups for SMEs: Korea.
- Provision of an online self-assessment tool for SMEs: United Kingdom.
- Developing software tools to facilitate the integration of electronic signature into SMEs' services and applications: Austria.
- Gathering statistics on the state of IT security in SMEs: Denmark.
- Offering financial assistance and tax support for fostering the production and procurement of secure systems: Japan.

12. The MCert initiative reported by Germany was presented in the « OECD Global Forum on Information Systems and Networks Security: Towards a Culture of Security » held in Oslo on 13-14 October 2003. See the proceedings in DSTI/ICCP/REG(2004)1.

Most successful initiatives and approaches used by governments for outreach to business and industry in order to foster a culture of security among business and industry and to develop public-private co-operation in various areas (Q8)

Almost all respondents report collaborative **awareness raising** initiatives. This result reinforces the findings of the 2003 survey: governments – as foreseen in the guidelines, and in the corresponding implementation plan –make awareness-raising a starting point for, and a central activity within their efforts to implement a culture of security. Collaborative activities across sectors are reported from some respondents. They are most frequent in the United States.

Many respondents also co-operate with business and industry with regard to **education and training**. Institutions tasked with such initiatives range from government agencies specialised in IT security, to law enforcement agencies (one example includes the local police force). Almost all respondents make training material available on the Internet. Other activities include seminars. One country (Spain) has set up a discussion forum on the Internet dedicated to security of information systems and networks.

In the March 2003 report of the US National Cyber Security Partnership Task Force on awareness and outreach, task force members (mostly from the private sector) provided their perspectives on best practices in education and awareness. They made suggestions for how a public/private national outreach awareness campaign could reach 50 million home users and small businesses in the US in the course of one year, through paid media, ISP's, security vendors, and other channels. The United States also report an initiative to define a job skill profile for security experts in the public and the private sectors. The United Kingdom is creating a new professional body for information security professionals.

Regarding **watch and warning and emergency response**, most respondents have CERTs or CERT-like institutions in place, some of which are operated by public private partnerships,[13] Most of these institutions target more specific audiences (*e.g.* the public sector, or a specific industry sector), while some are directed at the general public.

On **corporate Governance and ethics**, a few respondents report collaborative initiatives with the private sector. These include awareness-raising through Web sites and creation of a specific Committee (Japan), or hosting or co-hosting specifically tailored conferences (Germany). In the United States, one of the Task Forces of the National Cyber Security Partnership (NCSP) has published a report, which identifies cyber security roles and responsibilities within the corporate management structure, referencing and combining best practices and metrics that would foster accountability.

Many respondents have undertaken co-operative efforts with the business sector for the **creation and implementation of corporate security policies**. Some countries have made material (*e.g.* model policies or handbooks) available and are offering opportunities for voluntary certification (Austria, Germany). Korea posts criteria for security diagnosis on a portal site to be used by enterprises for self-testing. Norway has mandatory "ICT-regulations" for the financial sector. In Japan, the prefectural police is working with companies in critical infrastructure sectors to create corporate security policies.

No figures have been reported on the percentage of companies in the responding countries that have implemented corporate security policies, nor how having or not having a security policy impacts the frequency of security incidents in companies.

A few other co-operative efforts aim to **prevent and combat cybercrime**. Australia has formed an Investigations Team for the Banking and Finance sectors comprising staff from law enforcement and from

13. See also question 2.

the banking industry. Canada has a voluntary code of conduct for Internet Providers, and their public and private sectors co-operate in the ITAC Cyber Security Forum. Japan makes reference to preventive measures (tax incentives and a loan programme to foster production and application of secure systems and products, information material and seminars for businesses, analysis of Internet traffic data). Korea has created a national consortium of CERTs to foster co-operation among these institutions. Norway has established a cyber-crime unit in the Norwegian police. Another initiative in this context is the effort of the US Department of Justice to foster the underwriting of insurance policies covering cyber risks with insurance industry groups.

A few initiatives have also been reported regarding co-operative efforts across sectors for the **development of secure software**. Two countries have conducted or commissioned the development of secure software components related to digital signatures, involving co-operation between the public and the private sectors to different extents (Austria and Germany). Other countries promote research on secure operating systems (Japan – public sector), and on security incident response technologies (Korea). In one country (the United States) the government has promoted secure software development with industry. In addition, an agency of the Department of Homeland Security has developed a software assurance plan.[14]

A majority of respondents reported initiatives with respect to **technical standards and management standards.** The activities include the development of national standards in the area of information security, as well as co-operating on and participating in the further development of existing standardisation instruments at the international level. A number of respondents mention the use of national standards or methodologies for security certification of products, information systems and networks (*e.g.* Austria and Germany). However, no information was provided on whether these standards and methodologies are compatible with internationally recognised instruments.[15]

With respect to **independent certification of the security of information technology**, the standards most frequently referred to are the "Common Criteria" (CC or ISO/IEC 15408) and ISO/IEC 17799:

- The Common Criteria are mentioned by eight countries (Austria, Canada, France, Germany, Japan, Norway, Sweden, United States). Some countries mention the Common Criteria mutual recognition agreement.[16]
- ISO/IEC 17799 or corresponding national implementation is also mentioned by seven countries (Austria, Denmark – public sector, Finland, Norway, Portugal, Spain, United Kingdom).

Finally, certification functions for national standards or quasi-standards have been introduced, such as the German IT Baseline Protection Manual or the Austrian Security Handbook, in Japan, the ISMS scheme, in Korea, telecommunications provider certification and security "check-up", in Norway, financial sector ICT regulations and in the United States, cryptographic modules, in the United Kingdom, BS 7799 Part 2 – implementation of an information security management system.

No information was provided on how the existing certification approaches are received by users.

14. See also this item under question 4.

15. See also question 4.

16. . This agreement has been signed by 18 OECD countries.

Section V: Government as partner with civil society

Most successful government collaborative initiatives with, and outreach initiatives to, civil society to promote a culture of security for information systems and networks among users (Q9).

Almost all respondents report outreach initiatives to civil society. The majority list examples of initiatives taken by governments, in some cases in co-operation with the business sector, targeting citizens, *e.g.* aimed at raising awareness for emerging threats and countermeasures. Only a few respondents (Canada, Germany, Spain, United States) mention projects that would include partnering with institutions outside of government and business, *e.g.* with user groups. Some countries organise specific periodical events (information security day, or week) with actions to promote information security in the general public (Finland, Korea, United States). Finland has also established an interactive online government discussion forum for citizens and other participants.

Most successful government initiatives in the education system (pre-school age, all school ages, and higher education) to address the culture of security (Q10).

Eleven respondents report initiatives in the education system and four mention that no specific action has been taken in this area.

Most initiatives aim to educate children and students either through teachers, professors and parents or by direct distribution of guidance material. Only one initiative aims to target older persons. The support material varies from Web sites, games and online tools to postcards, textbooks and diploma. The initiatives include:

- **Teachers**: providing support material for teachers (Australia's NetAlert, Finland, Germany's "Schools go Online", Netherlands' "Cyber Secrets", United States' CyberSmart) and including security in the education programmes (Spain).
- **Children without Internet experience**: providing them with tools to play online while receiving educational messages related to information security (Australia's "Netty's World").
- **Children and youths with social handicaps**: providing them with a secure and pedagogically controlled access to the Internet (Germany's "Youths to the Net").
- **Children in general**: developing textbooks and games (Korea), creating an exam and a diploma (Netherlands's "Diploma Safe Internet"), a Web-based safe-surfer quiz (United States).
- **University and college students**:
  - Distributing material 160 000 "Dewie" postcards in 400 college campuses (United States).
  - Supporting students who write thesis (Germany), sponsoring a programme to produce a growing number of professionals with Information Assurance expertise (United States' National Centres of Academic Excellence in Information Assurance Education program and Scholarship for Service program, also called "Cyber Corps").
  - Developing policies for information security in universities (Canada).
  - Creating an e-card, compatible with the e-government scheme, to be used as ID-card, authentication, electronic signature device, room access card, copy card and electronic wallet (Austria).
- **Parents of young children**: delivering courses to inform them about security risks (Netherlands, United States' Cyber Smart).

- **Persons aged over 50**: providing basic information on how to use the Internet including security aspects (Germany's public-private-partnership "Initiative D21"), assisting middle-aged and elderly people to participate in the information society (Norway's Ministry of Modernisation and Ministry of Education and Research "Seniornett Norge" project, founded in 1997).[17]

Other initiatives have been mentioned such as:

- Establishing a competence centre for teaching and learning using new media at school (Germany).
- Maintaining a list of training courses provided by higher public educational institutions (France).
- Developing a CERT for educational institutions with a mandate to handle all cases of security incidents and disseminating security information (Netherlands' SURFnet-CERT, Finland's FUNET Cert for universities).

Australia and Finland have coupled initiatives targeting schools with events like "**Internet Security Day**". They also mention close **co-operation within regional initiatives** (Australia with the European Internet Safety Network (Insafe) and Finland with the dotSafe initiative from European Schoolnet[18]).

Partnerships and liaison with other participants (industry, consumer associations, educational organisations) were also mentioned by several countries (Australia, Netherlands, United States). In addition, Norway mentioned the SAFT (Safety, Awareness, Facts and Tools) regional initiative which involves five countries with the objective of "teaching children and teenagers how to reduce risk behaviour and be responsible Internet users". [19]

Section VI: Government efforts related to S&T and R&D

Science and Technology (S&T) and Research and Development (R&D) activities underway (or planned) (Q11). [20]

There is a consensus among responding countries concerning the pivotal importance of supporting R&D in order to find innovative information security solutions and approaches. *Ad hoc* programmes have been launched with government funds. The Netherlands has started the SENTINEL programme, whose objective is to develop secure applications for user-based systems, e-government and e-commerce. Meanwhile, France has launched the Oppidum initiative and Norway the IKT SoS. In several other countries (Austria, Denmark, Germany, Korea, Spain, United Kingdom, United States), information security projects are funded through regular national research programmes. Irrespective of their funding, these projects are focused on science and technology, with the exception of the Netherlands' SENTINEL, which examines also multidisciplinary issues.

17. Cf. www.seniornett.no.

18. www.dotsafe.eun.org, Schoolnet is an international partnership of more than 26 European Ministries of Education developing learning for schools, teachers and pupils across Europe.

19. Cf. www.saftonline.org. The following organisations are involved in SAFT: Norwegian Board of Film Classification, ICT Norway, MMI Norway, the Media Council for Children and Young people (Denmark), Home and School (Iceland), Council on Media Violence (Sweden), National Centre for Technology in Education (Ireland).

20. Possible areas listed in the questionnaire as examples in which government may have S&T and R&D activities were: vulnerabilities; best practices; security standards; development of secure software (*e.g.* methodologies); benchmarks and metrics for measuring the security of information systems and networks and the impact of respective initiatives.

Research activities are also supported by individual government organisations with information security responsibilities, such as the German Federal Office for Information Security, the Korean Information Security Agency, the Canadian Communication Security Establishment (CSE) and the National Cybersecurity Division within the US Department of Homeland Security (DHS). Their research activities, however, aim to either develop new solutions like RFID, biometrics or wireless solutions or to address immediate needs or concerns.

Responses also show that some countries facilitate the participation of industry and other independent research institutions in their information security research initiatives. This is the case in Spain, Germany, the Netherlands and Austria. Only some countries (Austria, Korea and the United States) report to have undertaken international information security R&D activities.

Section VII: Metrics and benchmarks

Metrics and/or benchmarks for measuring the impact and/or success of government's activities for Sections I-VI (Q12). [21]

Responding countries do not indicate that new metrics and benchmarks have been developed to assess their national information security policy. Three countries (Denmark, Finland, Norway), nevertheless, have separately started to develop and test indicators of a similar nature.

In three countries (Canada, Germany and Korea) national information security strategies are subject to the same standard evaluation processes as all other national policy initiatives. In Canada information security initiatives and processes are regularly audited and evaluated. In Korea, these initiatives are assessed according to the management by objective (MBO) methodology. In Germany, the achievements and progress of federally funded research initiatives are regularly monitored and assessed.

Finally, two countries (Germany and the United States) are assessing the level of awareness of information security risks in their country. Building upon the success of the annual Computer Security Institute /US Federal Bureau of Investigation (CSI/FBI) cybercrime survey, the US Department of Justice and Department of Homeland Security are currently surveying the information security status of 36 000 US businesses. In Germany, annual surveys regarding awareness of the products and services of the Federal Office for Information Security are undertaken with journalists, IT security officers and data protection officers. A similar "awareness monitoring" survey aimed at end users was carried out in 2004.

21. Related principles of the OECD *2002 Security Guidelines* for this question are: Security management, Reassessment.

ANNEX 1

COUNTRY SUMMARIES

This annex includes a summary of the responses, by country, which follows the structure of the questionnaire.

I. Government as developer of public policy, law, and regulation[22]

A. Comprehensive statement of strategy

Question 1: Development of a national policy and/or strategy on the security of information systems and networks and the promotion of a culture of security (process used to develop the strategy, nature and scope of the strategy, involvement and roles in policy development and implementation by the private sector, users and others).

Australia's strategy for fostering the security of the country's information systems and networks, while raising public awareness, emphasises the need to enhance public-private partnerships. In September 2001, the Australian government announced initiatives aimed at enhancing overall security knowledge and awareness in the private and public sectors, fostering the development of an e-security skill base, and encouraging R&D activities in this area. In November 2002, the government presented a set of initiatives for the protection of the country's critical infrastructures. At the core of these efforts is the Trusted Information Sharing Network (TISN), a forum of owners and operators of elements of the country's critical infrastructures. In case of an incident of a critical nature, the Information Infrastructure Protection Group, chaired by the Attorney General's Department, provides information and advice on how to protect the country's national information infrastructure.[23]

The E-Security Co-ordination Group co-ordinates the country's policy approaches to information security. Chaired by the Department of Communications, Information Technology and the Arts, this body brings together key policy, regulatory and law enforcement agencies. Its present priorities are overall awareness raising, information sharing between public and private bodies, research and development, and skill development. The activities of this body complement similar initiatives undertaken by TISN.[24]

Austria emphasises information security as one of the core elements of the country's e-government strategy. Under the leadership of the Federal Chancellor, an E-Government Platform has been set up to push e-government forward. Its activities are supported by an E-Co-operation Board, which brings together representatives of local, state and federal authorities. Furthermore, the ICT-Board agrees on strategic technical decisions and lays the foundations for comprehensive co-ordination of the ICT planning activities of the Federal Government. The Board is also tasked to report on progress and developments.

22. Questions 1-3 were primarily related to the policy-oriented principles (1-5) of the 2002 OECD *Security Guidelines.*

23. Cf. www.tisn.gov.au

24. See www.dcita.gov.au/ei/e-security

As detailed in the Information Security Act and a related decree, information security issues are addressed by the federal information security commission, headed by the information security officer of the Federal Chancellery. This body monitors overall compliance of the information security activities in each federal ministry, and co-ordinates their activities.

As part of its E-Government strategy, the Federal government directs particular attention to technical aspects of information security and privacy. The E-Government Act details issues like identity, privacy and secure delivery of official notices. Moreover, these technical implementations are seen as pivotal for supporting services and initiatives associated with the country's citizen card.

In April 2004, **Canada** issued the strategic framework and action plan *Securing an Open Society: Canada's National Security Policy* that *inter alia* puts forward an integrated approach to tackling present and future information security issues across the government. The action plan led to the establishment of a *National Cyber-security Task Force* with representatives from the private and public sectors. Nevertheless, the overall responsibility for the development and implementation of information security policy lies with the newly created Department of Public Safety and Emergency Preparedness, along with other federal departments and agencies.

The **Czech Republic** is in the process of developing national information security policies. It is expected to incorporate existing and international best practices in the areas of information security and the handling of classified information. The Czech Government has approved a State Information and Communications Policy ("e-Czech 2006").[25] The policy incorporates four priority areas, including affordable and secure communications services. In the area of electronic communications security, the Government provides active support to the deployment and practical use of advanced electronic signatures, as well as for other solutions increasing the security of electronic communications and enhancing the protection of privacy and personal data, and the observance of copyright and other statutory rights. Key objectives relating to electronic communications security include the establishment of a working group for combating computer crime, the development of the National Information Security Strategy, the operation of a reliable and secure communication network of public administration authorities, and the provision of smart cards to high- and middle-ranked civil servants. It is also planned to develop a security policy for information and network systems of the public administration. Ministries responsible for the area are: the Ministry of Informatics, the Ministry of Interior, the National Security Authority, the Office for Personal Data Protection, and the Ministry of Culture.

In **Denmark** the Ministry of Science, Technology and Innovation has established an IT security division within the country's National IT and Telecom Agency, and a Council for IT security.

The *IT security division* handles tasks associated with IT security policy at national and international levels, including relations with the OECD and the newly created European Network and Information Security Agency (ENISA).

The *Council for IT security* is an independent advisory body nominated by the Minister of Science, Technology and Innovation, aimed at fostering a culture of security and greater confidence in the use of IT systems and networks. Since its establishment, this body has drafted and distributed several booklets on security topics and has held several expert hearings to tackle new and challenging information security issues.

Finland's two overall key elements for the promotion of a culture of security are the Government Information Security Development Programme, and the National Information Security Strategy.

25. Available in English at www.micr.cz

In autumn 2003, the *Government Information Security Management Board* (VAHTI) set up a task force for structuring a plan for information security within the Finnish government. The implementation of the plan, which is consistent with the principles of the OECD guidelines, started in 2004. It involves six different areas ranging from the need to develop a culture of security within the government, to issues like data and communication security, the management of information security professionals, and support for service and process developers.[26]

At the same time, the Ministry of Transport and Communications prepared a government decision defining a National Information Security Strategy.[27] Its objective is to make Finland an information secure society by increasing citizens' and companies' online trust, and by fostering national and international co-ordination. As part of the national strategy, a *National Information Security Advisory Board* has been established. The Board monitors the implementation of the strategy and makes proposals for improvements and new challenges to the government.[28]

In **France**, the government considers that information security issues are essential for the success of e-government. In December 2003, the Prime Minister's Office approved the incorporation of the *State Information Systems Security Reinforcement Plan* in the *Administration Electronique 2004-2007 (ADELE) programme*, aimed to support e-government among the national administrations.[29]

Both the e-government and information security plans were officially launched in February 2004. The information security-focused plan aims at improving the security of government information systems, while preserving privacy of personal data and making information system security components operational. It also seeks to align France's information security policy with that of the European Union. In order to achieve these objectives, a set of specific measures have been put forward, ranging from raising security awareness, capabilities and training among senior government officials, to increasing the use of certified information security products.

In **Germany**, information security concerns are an integral part of national security, as confirmed by long-standing commitments to tackle these issues. Critical infrastructure protection is a particularly sensitive area since 80% of the nation's infrastructure is in the hands of the private sector.

Since 2002 the IT Staff Unit within the Federal Ministry of Interior (Office of the Chief Information Officer) focuses on information security. The bulk of the activities, nevertheless, is set within the remit of the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* - BSI). In addition to providing technical and operational support, BSI undertakes studies on future developments and trends in the information technology arena. This initiative provides the basis for the definition of future political decisions on information security and critical infrastructure protection.

In January 2000, **Japan**'s Interagency Director-General's Meeting on Information Security adopted an "*Action Plan for Information Systems Protection against Cyber-threats*". The goal of the plan is to foster information security in both public and private organisations. Building upon this action, the IT Security Promotion Committee, which brings together all ministries and agencies, adopted a "*Special*

26. Cf. www.vm.fi

27. The text is available at: www.mintc.fi/scripts/cgiip.exe/WService%253Dlvm/cm/pub/showdoc.p?docid=2099&menuid=180

28. The text of the first report of this body is available at: www.mintc.fi/scripts/cgiip.exe/WService=lvm/cm/pub/showdoc.p?docid=1735&channelid=26&channelitemid=9526&channelpubid=2

29. The text of the plan is available at: www.ssi.gouv.fr/site_documents/PRSSI/PRSSI-en.pdf

Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure Protection" (December 2000) and an "*Action Plan for Ensuring e-Government's IT Security*" (October 2001).[30] The status of the implementation of these plans is described in the 2003 and 2004 e-Japan Priority Policy Programmes.[31]

The Ministry of Economy, Trade and Industry (METI) established a *Comprehensive Strategy on Information Security* in October 2003. This was the first comprehensive information strategy in the country, with the objective to make Japan a highly reliable society through the implementation of 42 action items in both the private and public sectors.

In **Korea** the Ministry of Information and Communication (MIC) has been developing an Information Security Roadmap to support the country's IT839 strategy for Korea's long term IT development. The roadmap addresses 8 ICT services, 3 infrastructures and 9 new "growth engines", and approaches information security from a preventive perspective. To support its activities in this domain, the Ministry has established a *consultation body* comprised of experts from business, academic and research institutes, to foster the exchange of best practices and knowledge among the private and public sectors.

In the **Netherlands** information security policy involves three separate ministries:

- The Ministry of Economic Affairs is responsible for the general e-security policy and maintains international contacts with bodies like the OECD and the European Union.
- The Ministry of Interior is responsible for the protection of government information infrastructures and for e-government activities in general.
- The Ministry of Justice is responsible for addressing legislative aspects of information security.

Over the last years, information security has been the topic of a large set of policy documents and initiatives.

A 2001 study prepared by TNO (Netherlands Organisation for Applied Research) and Stratix identified key trends in Internet vulnerabilities and suggested policy activities aimed at fostering public awareness for better co-ordination in case of incidents.[32] Activities undertaken after the finalisation of this report include the KWINT programme (2002), which lead to the establishment of a government computer emergency response team (GOVCERT.NL), and of a national alert system for SMEs and private users.[33]

The Netherlands have also directed attention to the issue of critical infrastructure protection. Following the document *Action Plan Combating Terrorism and Security*,[34] the Ministry of Justice was asked to put forward a set of coherent measures. This has led to the *Protection of the Dutch Critical Infrastructure* project and a quick-scan exercise in 2003 that helped to determine interdependencies among the various critical infrastructures.[35]

30. Available at www.bits.go.jp/en/sisaku/cyber_terror.html and www.bits.go.jp/en/sisaku/h1310action.html

31. Cf. www.kantei.go.jp/foreign/policy/it/index_e.html

32. *Kwetsbaarheid op Internet* (KWINT) - *Samen werken voor veilig Internet verkeer* (TK 2000-2001, 26 643, no.30)

33. More information is available at: www.govcert.nl (Government CERT), www.nhtcc.nl (National High-Tech Crime Center - NHTCC), www.waarschuwingsdienst.nl (Alerting Service).

34. *Actieplan Terrorismebestrijding en Veiligheid* (TK 2001-2002, 27 925, no. 10).

35. *Bescherming Vitale Infrastructuur* (TK 2002-2003, 26 643, no.39).

Issues associated with information security were also discussed as part of the initiatives for fostering e-government activities, and in the 2004 *ICT Agenda*.[36] Moreover, at the beginning of 2005, the government started an internal project aimed at fostering information security professional skills defining potential economic incentives for information security, and fostering international co-operation and information sharing.

Norway's National Strategy for Information Security was initiated in 1998 when the State Secretaries' Committee for ICT identified the need to tackle growing concerns about information security. The process started with the establishment of a Vulnerability Commission to study the country's vulnerability associated with its dependence on information and communication technologies (ICT). Building upon the findings of this commission, a *National Strategy for Information Security* was put forward in 2000, and approved in 2003. Compliant with the OECD Security Guidelines, a comprehensive approach to information security is developed in the strategy as a basis for policy decisions and co-operation. It focuses on issues like the protection of critical infrastructures, the need to develop a culture of security, and enforcement and regulatory mechanisms.

The strategy currently in force in **Sweden** was presented in the Government Defence Bill in 2002.[37] The aim is to maintain a high level of information security in the whole of society, and to prevent or manage security problems in critical infrastructure and other key services in society. The strategy uses the same three principles as for other crisis management policies: Responsibility, parity, and proximity.[38] Those who are responsible for the operation of information systems must also assume the responsibility to have the appropriate level of security for the system. An important role for government is to look after the needs of society as a whole and take those actions that cannot reasonably be expected from individual system owners. Also, in order to avoid information attacks on Sweden, the Swedish Intelligence and Security Services were strengthened in this field. In the same bill the Government presented four additional information security tasks: (*i*) overall co-ordination and analysis; (*ii*) a technical support team; (*iii*) a CSIRT (CERT); and (*iv*) a system for IT security certification of IT products.

The Commission on Information Security currently evaluates the new tasks and the strategy, and will deliver its final report in September 2005. This Commission has a clear reference to the 2002 OECD *Security Guidelines* in its terms of reference. The overall responsibility to follow and oversee information security developments in central government agencies and other key parts of society lies with the Swedish Emergency Management Agency (*Krisberedskapsmyndigheten*, KBM) and its Infosec Division.[39]

36. ICT agenda (TK 2003-2004, 26 643, no.47)

37. The strategy was based on a report from the Swedish Commission on Vulnerability and Security that had in its remit to look at crisis management and civil defence in general. The Commission report and the other major studies used when the Government drafted its bill were all subject to the normal period of public consultation (usually three months) during which both the private sector and civil society were invited to comment, along with the relevant agencies.

38. Under the principle of responsibility, whoever is responsible for an activity under normal conditions, should assume corresponding responsibility in crisis situations. The principle of parity means that during a crisis, authorities should as far as possible be organised and located as under normal conditions. The principle of proximity means that crises should be dealt with at the lowest possible level.

39. The agencies' InfoSec Advisory Board consists of members from both the public and the private sector. It meets regularly to discuss and exchange information on current topics and policy developments. Strategic risk assessment is performed continuously by the agency during the year, and a report is produced on a yearly basis. Vital information infrastructures are identified through a strategic risk assessment. Cf. www.krisberedskapsmyndigheten.se/defaultEN____224.aspx

In the **United Kingdom**, a strategic approach to security of information systems and networks was developed by the Government following an internal review in 2003. The strategy is aimed at achieving the goal of information assurance, *i.e.* the confidence of having information available when it is required in the form it is required. It is primarily focused on ensuring that Government efforts are properly resourced and that there is direction and co-ordination of the Government's efforts. The strategy is aimed at improving the efficiency of Government, but acknowledges that the work of the Government in the field of information assurance needs to influence and be influenced by developments in the private sector. It is fully compatible with the OECD *Security Guidelines*. A "Central Sponsor for Information Assurance" (CSIA) was created as a unit in the Cabinet Office to oversee and co-ordinate inter-Departmental and inter-Agency activities in the field. While the strategy was negotiated within the Government, discussions with the private sector have taken place and the implementation of the strategy has deliberately drawn in a wide range of stakeholders on some more specific goals, for example with regard to outreach, or professionalisation of information security experts. A publication was issued by the CSIA to draw the attention of all stakeholders to the underlying themes of the strategy and its relevance for all users.[40]

In February 2003, the **United States** issued a National Strategy to Secure Cyberspace and created a National Cyber Security Division within the Department of Homeland Security (DHS) for its implementation. Based on consultation with industry and civil society, the Strategy identifies five national priority areas:

- Development of a national cyberspace security response team.
- A threat and vulnerability reduction programme.
- A national cyberspace security awareness and training programme.
- E-government security.
- National and international information security co-operation.

Portugal, the **Slovak Republic** and **Spain** are planning to develop information security strategies over the next months.

B. Legal, regulatory, and institutional arrangements to oversee and implement a culture of security

Question 2: Legal, regulatory and institutional arrangements to implement a culture of security (Nine areas identified: Cybercrime; Computer incident watch and warning, and response; Critical infrastructure; Risk assessment; Outreach to business, civil society and others; Outreach to state and local government; Education and training; Science and technology (S&T) and research and development (R&D); International outreach and co-operation[41]*).*

a) Cybercrime

Australia reports to have a comprehensive national regulatory framework in place to address business and community concerns about using the Internet for conducting business, including the *Cybercrime Act*

40. www.cabinetoffice.gov.uk/csia

41. For each area: detail on the arrangements and implementation, including division of responsibilities, among various government bodies; international co-operation and information sharing, and provide points of contact for international co-operation and information sharing; incorporation of existing and developing international best practices.

2001,[42] and the *Crimes Act 1914.*[43] The key offences in the Cybercrime Act 2001 are consistent with the Council of Europe's 2001 Convention on Cybercrime.

The Government established the *Australian High Tech Crime Centre* (AHTCC)[44] in July 2003 to combat instances of high tech crime impacting on the Australian jurisdiction and co-ordinate cybercrime fighting efforts between various state and Government agencies. The AHTCC consists of police investigators, intelligence analysts and seconded personnel from a range of government regulatory organisations and the private sector. Its role is to: (*i*) provide a co-ordinated national approach to combating high tech crimes of a serious, complex and/or multi-jurisdictional nature, generally beyond the capability of one jurisdiction; (*ii*) create a centre of knowledge and expertise to assist all jurisdictions in building their high tech crime capacity; (*iii*) conduct intelligence-led policing and best application of scarce and specialised policing resources, both human and technical; (*iv*) work co-operatively and in partnership with all national and international law enforcement agencies, and other key stakeholders including government regulatory agencies and the private sector; (*v*) develop strategic alliances and partnerships with key agencies and organisations (including the private sector, academia, and industry associations); and (*vi*) develop mechanisms to protect the national information infrastructure.

The AHTCC engages with private sector organisations to build a private/public partnership to combat high-tech crime, including secondments to the AHTCC from private sector organisations to conduct investigations, share intelligence and build capacity. The AHTCC has also conducted a range of training initiatives designed to improve the knowledge and capacity of the Australian Police to investigate instances of high-tech crime. This training has also been extended to some Commonwealth regulatory agencies.

The **Austrian** Penal Code implements the regulations of the CoE cybercrime convention, such as: (*i*) destruction of data [*Datenbeschädigung* - section 126a]; (*ii*) disruption of computer system functioning [*Störung der Funktionsfähigkeit eines Computersystems* – section 126b]; (*iii*) abuse of computer programs or login data [*Missbrauch von Computerprogrammen oder Zugangsdaten* – section 126c]; or (*iv*) fraudulent misuse of data [*Betrügerischer Datenverarbeitungsmissbrauch* – section 148a]. Many cases of cyber fraud are covered under existing penal regulation on fraud, and do not require special legislation.

The *National Computer Crime Unit – Austria*, part of the *Bundeskriminalamt* (Criminal Intelligence Service Austria) comprises four sub-departments with different responsibilities. This department in the Ministry of Interior is a central point for the combat against computer crime, with staff especially educated and trained. The main areas of work are crimes with illegal and actionable attacks on computers (*e.g.* hack or virus attacks) or crimes where computers are used for illegal actions (*e.g.* fraud), based on the Austrian Penal Code. Investigators are taking action when they are notified about a crime from any executive authority. The unit is working closely with Interpol. In case of an IT-crime, the information can be securely exchanged over the Internet with other national and international security authorities. The unit represents Austria in the European Network of Forensic Science Institutes on Computer Crime (ENFSI).

The Criminal Code of **Canada** contains provisions against misuse of computer systems, or tampering with an information system. It targets hacking into protected information stored on computers, spreading of malicious viruses, and launching denial of service attacks. In the case of all other substantive criminal activity, such as fraud committed using a computer, Canadian law does not distinguish between computer mediated and off-line criminal activity. As a signatory to the Council of Europe Convention on Cybercrime, Canada is developing new tools to assist law enforcement agencies in the investigation of the misuse of information technologies. The *Information Technology Association of Canada* leads an industry

42. www.policensw.com/pdf/161of2001.pdf

43. www.scaleplus.law.gov.au/cgi-bin/download.pl?/scale/data/pasteact/0/28

44. www.ahtcc.gov.au/

forum that promotes information sharing on domestic and international issues and the development of technological solutions to cyber attacks.

The **Czech Republic** has a *National Action Plan to combat terrorism*,[45] covering basic objectives to be fulfilled to increase the preparedness against possible terrorist attacks in the country and abroad.

Denmark has a National Police Unit for fighting IT crime.

Finland has legislation on criminal activities on networks and computer systems, and a national police unit for fighting IT crime.

France has a legal framework in place to ensure the security of information systems. In 1988, the so-called *Godfrain Law* supplemented existing criminal provisions by imposing penalties for acts of vandalism against information systems, and provided a judicial arsenal against computer crime such as viruses, logic bombs and "Trojan horses". In addition, *Act No. 2004-575 of 21 June 2004 for confidence in the digital economy* increased penalties for fraudulent access to an automated data processing system, for impeding or distorting the operation of such a system, and for fraudulently entering or deleting data. These regulations are consistent with the Council of Europe Convention on Cybercrime. France is a signatory to the convention (2001), and has almost finished the ratification process (an act was adopted in May 2005 authorising the ratification of the convention). France also supports the finalisation of the "European framework decision on attacks against information systems", currently under discussion in the Council of the European Union.

In order to fight more effectively against cybercrime, in May 2000 France established the *Central Office for Combating Crime Involving Information and Communications Technologies* (OCLCTIC).[46] The two main missions of the Office are: (*i*) to conduct judicial investigations that require a high level of competency with respect to information technologies; and (*ii*) to provide training, and co-ordinate actions with other law enforcement agencies having jurisdiction over IT-related offences.

In **Germany**, the *Second Law on Combating White-collar Crime* introduced in 1986 provisions of IT-related criminal law to the German Criminal Code: (*i*) Criminal offences against the confidentiality, integrity and availability of computer data and systems;[47] and (*ii*) Computer crimes using computer and telecommunications systems for the purpose of launching new forms of attack against certain objects protected by law.[48]

---

45. The plan was approved through the Czech government resolution No. 479 of 19/6/2004. Cf. www.mvcr.cz/aktualit/sdeleni/2002/nap/nap_eng.html

46. OCLCTIC is part of the Central Directorate of the Judicial Police (DCPJ) within the Ministry of the Interior. Staffed with police officers and gendarmes, it performs special surveillance of Internet transactions and fosters close co-operation with Internet service providers for the detection of "paedo-pornographic" Web sites. Cf. www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic.

47. These include criminal offences concerning the unauthorised capturing and exploitation of data (data, computer espionage, sections 202a of the German Criminal Code (*Strafgesetzbuch* - StGB), 17 subsection 2 of the Law against Unfair Competition (*Gesetz gegen unlauteren Wettbewerb*), and attacks against the integrity of data and computers (sections 303a, 303b, 274 subsection 1 No. 2 of the German Criminal Code).

48. These include criminal offences, such as forgery of data serving as evidence (sections 269, 270 of the German Criminal Code), computer fraud (section 263a of the German Criminal Code) and other content-related criminal offences, such as the dissemination of propaganda by unconstitutional organisations (section 86 of the German Criminal Code), presentation of violence (section 131 of the German Criminal Code) and the dissemination of pornographic writings (sections 184 seq. of the German Criminal Code). Section 11 subsection 3 of the German Criminal Code provides that data storage media are to be treated like written documents, so that cases of dissemination through electronic data networks are covered.

Germany co-operates in international organisations for fighting cybercrime, such as the European Union, the Council of Europe and within the G8 group.

The Council of Europe Convention on Cybercrime (CETS 185) and the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature (CETS 189) were signed by Germany on 23 September 2001 and 28 January 2003, respectively. The federal government is planning to take action to implement this convention – in particular, amendments to material criminal law – during the present parliamentary term. The implementation law is also to cover amendments resulting from the EU draft framework decision on attacks on information systems. The additional protocol mentioned above will be ratified following the ratification of the mother convention.

Investigation tools available under criminal procedure law include telecommunications surveillance pursuant to sections 100a, 100b of the German Code of Criminal Procedure (*Strafprozessordnung* - StPO) and connection data retrieval pursuant to sections 100g, 100h of the Code of Criminal Procedure.[49]

Organisational units have been set up to prosecute cybercrime both at the federal states' police organisations and at the Federal Criminal Police Office, with the technical knowledge and skills required for criminal investigation in cases of criminal offences related to information and communication technology. In 1999, an additional central unit was established at the Federal Criminal Police Office responsible for prosecuting criminal offences in data networks. This *Central Unit for Suspicion-independent Research in Data Networks* (*Zentralstelle für anlassunabhängige Recherche in Datennetzen* (ZaRD)) scans the Internet and online services for criminal content, and further prosecutes facts of criminal relevance discovered during the course of this research, including collection of evidence and identification of offenders. It also performs research into specific criminal cases as a parallel task.

The *Federal Criminal Police Office*, also responsible for investigating serious cases of computer sabotage and attacks on critical infrastructures, provides specialist technical support for investigators when it comes to prosecuting criminal offences on the Net and attacks on critical IT infrastructures. To this effect, the office not only carries out real investigation work, but is also actively developing and upgrading methodologies.

In the framework of the *Initiative D21*[50], together with D21 member companies and representatives of the relevant investigation authorities, questions and concepts are being developed in order to combat fraud on the Internet efficiently. Promoting better co-operation between public authorities and providers is one of the key tasks of this project group. The project aims to establish trust-forming and information measures.

---

49. Pursuant to sections 100a, 100b of the Code of Criminal Procedure, law enforcement authorities are authorised to tap and record communications via data networks, such as the Internet, in real time. Pursuant to sections 100g, 100h of the Code of Criminal Procedure, telecommunications service providers must on demand disclose to law enforcement authorities any connection data stored with regard to such communications. Since the connection data includes the IP address of a computer, it is thus, for example, normally possible to identify the computer from where an e-mail was sent. These provisions are currently undergoing comprehensive revision also with a view to enabling even more effective combating of cybercrime and offences committed or substantially supported by the use of computers. Besides the above-mentioned legal provisions, sections 94, 95 of the Code of Criminal Procedure allow for confiscating data volumes which can serve as evidence in criminal proceedings.

50. The “Initiative D21” is Germany's largest Public Private Partnership composed of more than 400 representatives from industry, associations, political parties, political institutions and other organisations. Its aim is to improve the national framework for the information and knowledge society in order to boost Germany's international competitiveness. Cf. www.initiatived21.de

Japan has introduced substantive and procedural legislation in the area of cybercrime through (*i*) Enforcement of the unauthorized computer access law; (*ii*) Enforcement of the law concerning the regulation of acts inducing children using the Internet dating services and other matters; and (*iii*) Revision of domestic laws for the ratification of the Council of Europe Convention on Cybercrime. The bill is now being deliberated in the Diet.

With respect to enforcement, the *National Police Agency* (NPA) has in April 2004 established a cybercrime division in charge of policy making and co-ordination of both investigation and prevention of cybercrime. Each prefectural police has a *counter-cybercrime group* composed of competent experts. Each prefectural police reinforces cybercrime investigation and prevention by hiring information security experts from industries as *cybercrime investigators*, for training police officers to cope with cybercrime and improving equipments for cybercrime investigation. In terms of technical assistance and technical analysis, NPA established the *Cyber Force* in 2001, mobile technological units at the national and regional levels, to provide technical assistance and analysis to prevent and mitigate damages from cyber terrorism. They carry out efforts on a 24/7 basis to detect signs of cyber terrorism and identify potential incidents at an early stage. Moreover, the NPA has also established a *High-tech Crime Technology Division* in each Prefectural Info-Communications Department in 2004, to enhance the capability of technological support to cybercrime investigators.

As regards prevention, a report on research and development with regard to access control technology is annually published by NPA, the Ministry of Internal Affairs and Communications (MIC) and the Ministry for Economy, Trade and Industry (METI). In addition, METI, IPA and JPCERT/CC[51] publish Computer Virus / Unauthorized Computer Access Incident Reports, operate a *Traffic Monitoring System* on the Internet, and a *Vulnerability Handling Framework*. NPA publishes information about the current situation of cybercrime, its countermeasures and policy of NPA through the NPA *counter-cybercrime Web site*,[52] and has set up a *security portal site* '@police'[53] in order to quickly provide technical information gathered by the police on information security for the purpose of preventing cybercrime and cyber terrorism. In addition, each prefectural police provides information through *Information Security Community Centers* together with other PR activities through various media, and holds *Conference Calls with Internet Service Providers* to exchange information about cybercrime trends and methods.

In **Korea**, the *Public Prosecutor's Office* and the *National Police Agency* conduct the criminal investigations. Investigative bodies for cybercrime are the *Internet Crime Investigation Centre*[54] and the *Cyber Terror Response Center*.[55] ISPs are required by law to report incidents of cyber attacks to the authorities, and preserve the related documents. As the threats to the information and communication networks are increasing, the Ministry of Information and Communication (MIC) has established the *Framework Act on Telecommunications*, the *Act on Promotion of Information and Telecommunication Network Utilisation and Information Protection*, the *Act on Protection of Information and Telecommunication Infrastructure*, etc. Based on these Acts, it established in 1996 the 'Korea Information Security Agency (KISA)' to implement the information security policies in the private sector.

In the **Netherlands**, the *Computer Crime Act* of 1993 contains a number of provisions regarding various types of computer-related crimes, such as hacking, unauthorised entering of computer systems and

51. The Japan Computer Emergency Response Team Coordination Center.

52. www.npa.go.jp/cyber/

53. www.cyberpolice.go.jp

54. http://icic.sppo.go.kr/main_english.htm

55. http://ctrc.go.kr/english/main.jsp

destruction of data.[56] In July 1999 a follow-up Bill, the *Computer Crime Act II*, was introduced in Parliament. This act will refine and update several provisions of the Computer Crime Act I. However, as a result of the delayed Convention on Cybercrime (CETS 185, finalised by the Council of Europe in 2001, which became effective in 2004), the implementation of the Convention into Dutch law together with the revisions recommended in the Computer Crime Act II Bill are still in preparation. Along the lines of European legislation in the field of cybercrime, the Dutch legislation identifies two categories of high-tech crime: *i*) criminal offences against the confidentiality, integrity and availability of computer data and systems: identity theft, hacking, cracking, viruses, denial of service attacks, spyware; and *ii*) traditional crime in which computers or information and communication networks play a facilitating role: fraud, drug dealing, child pornography, threat, discrimination.

Police and Justice recognise the difficulties involved in prosecuting and solving these sorts of crimes. Currently, a few police officers have the specific technical expertise that is needed to estimate the value and impact of high-tech crime. Also, the division of responsibilities complicates the operational investigation and prosecution of cybercrime. Although there is a team of 200 highly qualified digital experts working within the police force, these people are not always deployed in the most effective and efficient ways, being spread across the 26 regional police forces, which all operate independently. After publication of its report on the national project "Digital Investigation" in September 2004, the government started to implement some of the recommendations from the report, including changes in the organisation of the police force, and education of personnel, to adapt to the reality of high-tech crime. In 2005, the National Crime Control Platform embarked on a strategic policy project entitled Approach of Cybercrime (*Aanpak Cybercrime*). This project aims to clarify the needs, roles and responsibilities of government and industry in the fight against cybercrime.

Another initiative designed to streamline the combating of cybercrime is the *National High-Tech Crime Center* (NHTCC; www.nhtcc.nl), involving the Ministries of Justice, Interior, and Economic Affairs, together with the KLPD (the national police agency). It set up a centre in late 2004 with a facilitating role in cybercrime investigation and prosecution. This centre also collects knowledge and expertise on high-tech crime to be able to give advice on prevention. The NHTCC aims at providing early warning and effective response to serious crimes involving ICTs. It focuses on the impact of cybercrime on the Dutch society, and on vital information infrastructures in particular.

In **Norway**, a *cyber-crime unit* has been established in the Norwegian police. The Norwegian Post and Telecommunication Authority (NPT) participates in a *working group on legal interception.*

In the **Slovak Republic**, the implementation of the content of the Convention on Cybercrime of the Council of Europe is in progress, and is expected to result in a revision of the Criminal Code.

Spain has criminal legislation on cybercrime in place, consistent with the Convention on Cybercrime of the Council of Europe. The National Police[57] and the Civil Guard[58] have *specialised units* fighting cybercrime.

---

56. This Act resulted in a number of adaptations of several sections in the Telecommunications Act, the Dutch Criminal Code and the Code of Criminal Procedure. Legislation on cyber security (prevention), concerning the integrity, availability and reliability of electronic networks and services has been defined in the Telecommunications Act, whereas legislation on cybercrime (prosecution), concerning breaking into computer systems and electronic networks and manipulation of data, has been laid down in the Criminal Code and the Code of Criminal Procedure.

57. www.mir.es

58. www.guardiacivil.org

Sweden is in the process of implementing the CoE Cybercrime convention and relevant EU frameworks to deal with cybercrime. The Swedish National Criminal Investigation Department has together with the Swedish Security Service set up a special unit to co-ordinate and deal with reported cybercrime. They also provide information on prevention and support local police forces in investigating IT related crimes.[59]

In the **United Kingdom**, the key legislative instrument regarding attacks against computer systems and data is the Computer Misuse Act of 1990 which outlaws the unauthorised modification of data stored or transmitted by IT systems, as well as unauthorised access to such systems. The legislation is drafted in general terms and is regularly used as the basis for prosecutions of hackers and those who disseminate viruses or worms. There is a range of other legislation in the UK dealing with offences utilising computer systems and networks, for example using computers or the Internet to facilitate fraud is covered by offences in fraud legislation. The UK intends to ratify the Council of Europe Convention on Cybercrime in due course.

Enforcement is carried out at two levels: The National High Tech Crime Unit (NHTCU[60] a national expert police unit which is part of the UK's National Crime Squad) is responsible for combating serious and organised computer criminality. It provides strategic assessments, operational and tactical support, business intelligence and best practice advice for constabularies. The NHTCU also has a strong role in crime prevention and engages actively with the likely victims of crime — such as the financial institutions — to share information on actual and possible criminal activities. A Confidentiality Charter was developed and launched in December 2002 to help business to interact with the NHTCU in a secure, efficient and confidential manner when wishing to exchange information, report hi-tech crime, or seek advice. The main operational policing responsibility for investigating computer crime rests within the specialist cybercrime units which have been established within every constabulary (a police force based largely on County and large Metropolitan boundaries). The UK Government has provided additional funding to provide staffing, training and equipment in every local police constabulary in England and Wales to supplement the expertise in their specialist cybercrime unit.

In the **United States**, the *Department of Justice* (DOJ) is the prosecutorial arm of the Executive branch of the federal government, and has devoted significant resources to investigating and prosecuting persons who commit crimes on the Internet. The DOJs Criminal Division's *Computer Crime and Intellectual Property Section* (CCIPS) is comprised of experienced, technology-trained prosecutors who co-ordinate investigations into all types of cybercrime, including intellectual property crime, both domestically and internationally. In addition to CCIPS, there are more than 220 technology prosecutors located throughout the 94 federal law enforcement districts to ensure that high-tech expertise is brought to bear on computer crime investigations. These resources are supplemented by a cadre of specialised *Computer Hacking and Intellectual Property (CHIP) units* located in strategic districts across the country. The CCIPS is also the point of contact for the Group of Eight (G-8) 24/7 hi-tech network, which currently includes 40 countries, through which requests for immediate police or prosecutorial assistance can be made 24 hours a day, 7 days a week.

In 1984, the United States Congress passed the first federal law that prohibited unauthorised access to computers and other criminal conduct related to computers. Since then, US law has undergone significant amendment to expand the applicability of criminal laws to new and emerging challenges in computer crime, and to increase the penalties for the most serious violations of the law. Today, US federal computer crime law includes both substantive provisions that address a wide range of computer crimes and

59. For information about the Swedish Police cf. www.polisen.se/inter/nodeid=10230&pageversion=1.html; Swedish Security Service: www.securityservice.se/

60. www.nhtcu.org

procedural tools that permit law enforcement investigation of criminal conduct while respecting individual privacy. In addition, US law provides for mutual legal assistance through formal requests for assistance either by treaty or letter rogatory as appropriate. As such, US law is in compliance with the provisions of the Council of Europe's Convention on Cybercrime. Upon the referral of the President, the Convention on Cybercrime is presently before the United States Senate for its advice and consent to ratification.

The principal US federal law to combat cybercrime is the *Computer Fraud and Abuse Act* (18 USC. § 1030) ("CFAA"). The CFAA addresses a wide range of cybercrime and criminalises the following conduct: (*i*) intentionally accessing a computer without authorisation or exceeding authorisation and obtaining information; (*ii*) intentionally accessing a non-public computer used exclusively by the US government; (*iii*) knowingly, and with intent to defraud, accessing a computer without authorisation or exceeding authorisation and obtaining anything of value; (*iv*) knowingly causing the transmission of a program, information, code, or command and intentionally, recklessly and in some cases, negligently causing USD 5 000 or more in damage, or results in the modification or impairment of medical information; physical injury to any person; a threat to public health or safety; or damage to a computer system used by a government entity in furtherance of the administration of justice, national defence, or national security; (*v*) knowingly and with intent to defraud trafficking in passwords or similar information through which a computer may be accessed without authorisation; and (*vi*) transmitting a threat to cause damage to a computer with the intent to extort money or any thing of value from any person.

The Federal Bureau of Investigation (FBI) is the investigative division of the Department of Justice. The FBI's *Cyber Division* is the lead law enforcement agency for investigating cyber attacks by cyber criminals. The FBI also works to prevent criminals, sexual predators, and others intent on malicious destruction from using the Internet and online services to steal from, defraud, and otherwise victimise citizens, businesses, and communities. The mission of the FBI's Cyber Division is to: (*i*) co-ordinate, supervise and facilitate the FBI's investigation of those federal violations in which the Internet, computer systems, or networks are exploited as the principal instruments or targets of cybercrime; and (*ii*) form and maintain public/private alliances in conjunction with enhanced education and training to maximise counter-terrorism and law enforcement cyberresponse capabilities. The FBI also maintains the *Internet Complaint Center* to facilitate the reporting of cybercrime and is the lead investigative agency in several initiatives directed to cybercrime such as spam, Internet fraud, and "phishing."

The US law enforcement community has also created a mechanism for sharing information with known partners in the DHS/USSS *Electronic Crimes Task Forces* (ECTFs). The ECTFs bring together representatives from federal, state, and local law enforcement, academia, and the private sector, and are based in major metropolitan areas with a focus on the specific needs of the surrounding community.[61] In smaller metropolitan areas, DHS/USSS has initiated eight smaller Electronic Crime Working Groups (ECWGs).[62]

61. For example, the ECTF in Charlotte, NC has significant representation from the banking and finance community, while the San Francisco ECTF focuses more on the high-tech industry. This individualisation of the task force leads to increased participation from local private industry and academia. Through daily interaction and joint investigations, trust relationships are formed that allow for better information exchange and co-operation. As a result of the success of these groups, DHS has authorised an increase in the number of ECTFs from 9 to 14, including a European task force.

62. ECWGs similar to ECTFs, but they recognise the unique nature of the community they serve.

b) Computer incident watch and warning, and response

Australia has a national technical *Computer Emergency Response Team* (AusCERT), a non-government, not-for-profit organisation. Following negotiations with the federal government, AusCERT provides a *National Information Technology Security Reporting and Alert Scheme.*[63]

Austria has founded the *Computer Incident Co-ordination Austria* (CIRCA),[64] a public/private partnership designed as an information and action network at the national level, composed of multidisciplinary incident experts from ISP, IT-security firms, critical infrastructures, companies with big networks and organisations from the public sector. Communication means in place give the opportunity to react and act immediately in the case of severe incidents. To speed up the process of recognising critical situations at an early stage, a sensor concept is used. The three main players involved are the Federal Chancellery, the "Internet Service Providers Austria" (ISPA)[65] and the "Secure Information Technology Center" (A-SIT).[66]

The **Canadian** federal Department of Public Safety and Emergency Preparedness (PSEPC) has recently established a *Canadian Cyber Incident Response Centre* (CCIRC) which will serve as the focal point for dealing with cyber threats and incidents impacting Canada's critical infrastructure 24 hours a day, 7 days a week. The CCIRC will co-ordinate strategic incident responses, monitor and analyse the cyber threat environment, provide warnings and technical advice and finally, increase national awareness and capacity building.

PSEPC has also developed a *National Exercise Program*, designed to enhance emergency management operational readiness, including cyber protection, by promoting, facilitating and co-ordinating exercises involving federal departments, provincial, municipal, international and private sector partners. A private sector company (EWA Inc.) has been operating a *Canadian Computer Response Team* ("CanCert") since 1998. The initiative functions as a trusted centre for the collection and dissemination of information related to networked computer threats, vulnerabilities, incidents and incident response for government, business and academic organisations. Both CCIRC and CanCert are part of a worldwide network of CERTs that collaborate and share security-related information on a 24/7 basis.

The *Information Technology Association of Canada* leads an industry forum that promotes information sharing on domestic and international issues and the development of technological solutions to cyber attacks.

In **Finland**, CERT-FI (the Finnish Computer Emergency Response Team), an institution of the Communications Regulatory Authority (FICORA), publishes security alerts on acute security threats and measures to tackle those threats. In addition to alerts CERT-FI also publish information security advisories aimed at informing end users on current developments in information security. Alerts and advisories are available via Web pages, e-mail and text-TV.

In **France**, the *Expert Government Response Centre for the Treatment of IT Attacks* (CERTA) was established on 19 January 1999 as an Internet alert and assistance centre, to provide assistance to government agencies victimised by computer-related incidents or attacks. Operational since year-end 1999 as part of Y2K preparedness measures, CERTA has been assigned to perform technology monitoring of all

63. www.national.auscert.org.au

64. Cf. www.circa.at

65. Cf. www.ispa.at

66. Cf. www.a-sit.at

new types of attacks and system vulnerabilities, to alert government agencies in the event of serious IT attacks or discovery of new vulnerabilities, and to oversee the resolution of computer incidents in government agencies. Composed of some 15 high-level technical experts, CERTA is part of the *Central Directorate for Information Systems Security* (DCSSI). It publishes four different types of documents which are available on its Web site and are disseminated to administrators of information systems: (*i*) "Opinions", providing a brief description of a vulnerability, its consequences, and means of protection (generally a software patch); (*ii*) "Alerts", providing advice if no patch has yet been issued and measures need to be taken rapidly; (*iii*) "Information notes", providing detailed explanation of security-related topics; and (*iv*) "Recommendations" on organisational measures. The targeted audience are public-sector information system security managers responsible for the security of their own networks. All documents produced by CERTA are available on its Web site.[67] CERTA is a member of three international organisations of CERTs, the TF-CSIRT,[68] FIRST,[69] and the European CERTs Group (EGC).[70] Furthermore, there are two other CSIRT institutions operating in France.[71]

Germany operates a CERT for the Federal Government (CERT-Bund). IT security issues in the context of the introduction of new IT solutions in the Federal administration are co-ordinated through an advisory board.[72] The Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – BSI)[73] is the central IT security service institution in the country. It has wide ranging responsibilities with respect to fostering information security at the national level. For example, BSI provides advisory services for the administration, business and the general public, and targets professionals as well as private users.[74]

In **Japan**, the *Telecom-ISAC Japan* was established in July 2002 by Japanese ISPs and vendors as a private organisation that collects, analyses and shares security information among its members. Furthermore, the Ministry for Economy, Trade and Industry (METI), the Information-technology Promotion Agency (IPA) and JPCERT/CC[75] have implemented a scheme of *Computer Virus / Unauthorized Computer Access Incident Reports*, a *Traffic Monitoring System* on the Internet, and a *Vulnerability Handling Framework.*

67. Cf. www.certa.ssi.gouv.fr/index.html. In 2003, CERTA published 25 alerts, 859 opinions, and 1 information note.

68. In 2003, TF-CSIRT comprised 79 computer security incident response teams (CSIRTs) in 30 countries, whose missions are to: (*i*) Create a European model for "ensuring the level of confidence"; (*ii*) Create a common "incident description" language; (*iii*) Insert a security contact point (IRT object) into the RIPE database; and (*iv*) Formulate a suitable training scheme for CSIRTs and assist in the creation of new CSIRTs.

69. FIRST comprises more than 170 teams in Europe, the Americas, Asia and Oceania. It aims to: (*i*) Foster co-operation between CSIRTs; (*ii*) Provide joint communications capabilities; (*iii*) Assist members in developing their activities; and (*iv*) Facilitate the sharing of information.

70. The EGC covers European governmental CSIRTs.

71. For example, Cert-IST is a dedicated CERT for the industry, services and tertiary (IST) sector. It was set up at the end of 1998 by four partners: Alcatel, CNES, ELF and France Télécom. CERT-RENATER is the dedicated CERT for the community of GIP RENATER members (National Telecommunications Network for Technology, Education and Research).

72. The "Coordination and Advisory Board of the Federal Government for Information Technology in the Federal Administration (KBSt).

73. www.bsi.bund.de

74. www.bsi-fuer-buerger.de

75. The Japan Computer Emergency Response Team Coordination Center.

In cases of cyber-terrorism, the National Police Agency (NPA), the Regional Police Bureaus and Prefectural Polices establish an *ad hoc* body to respond, prevent the expansion of damage caused by the incident, and conduct investigations. NPA also provides warnings and information on the current state and signs the spreading of viruses/worms, and of other malicious activities on the Internet to the public through content on the NPA security portal site '@police', such as 'Internet Activities Monitored' and 'Malicious Activities on the Internet'. This information includes analysis of data collected from intrusion detection systems (IDS) and firewalls installed at police institutes nationwide.

In **Korea**, a response system has been established with the *Korea Internet Security Centre* (KrCERT/CC[76]) within the Korea Information Security Agency (KISA) in December 2003, to respond to Internet security violations in the local private sector, to security breaches on a global scale, and to build a uniform co-ordination system with Internet operation agencies. KrCERT/CC conducts 24/7 Internet backbone monitoring in co-operation with major ISPs, IDCs and MSSPs (Managed Security Service Provider). They provide real-time statistical information on Internet traffic, such as BPS, PPS for the line and high ranking ports, and on cyber attacks such as high ranking attack types. This co-operation relationship used to be based on agreements among stakeholders at first, and is now imposed as a legal obligation (The Act on Promotion of Information & Communication Network Utilisation and Information Protection, etc). Furthermore, the centre analyses vulnerabilities detected in hard- and software, and the influence of new versions of viruses and worms, in order to be able to respond in a timely manner to Internet security breaches. It also develops response measures by studying and analysing recent hacking methods, provides technology support, and acts as a channel for international information exchanges by operating the "Consortium of Computer Emergency Response Team" (CONCERT),[77] and by participating in international organisations such as FIRST and APCERT.[78] Twenty-five ISPs and controlling businesses conduct regular monitoring to identify unusual traffic, and provide information on network operation. Legislation requires ISPs to report incidents of cyber attack to law enforcement angencies, and to preserve related documents or data. To strengthen regular security activities and support the establishment of information security management systems, the government has made it *mandatory for companies to undergo security check-ups* under the existing information security guidelines.

In the **Netherlands**, the Computer Emergency Response Team for the government was set up in 1992, and is known as GOVCERT.NL (www.govcert.nl). GOVCERT.NL is the government's central reporting and co-ordination centre for ICT-related security incidents. Its objective is the prevention and handling of ICT-related security incidents for national, regional and local government institutions and agencies as well as SMEs and consumers. It is responsible to the Ministry of the Interior and Kingdom Relations; its activities are co-ordinated by ICTU, the ICT organisation of the public sector.

GOVCERT.NL[79] has a comprehensive international network for the sharing of information and expertise in the development of international standards. It is a member of international partnerships, including the EGC,[80] FIRST,[81] TERENA,[82] I4,[83] and the Information Security Forum (ISF). At the national level, GOVCERT.NL co-operates with SURFnet-CERT.[84]

76. www.krcert.org

77. www.concert.or.kr

78. The Asia Pacific Computer Emergency Response Team – APCERT – is an association of Computer Security Incident Response Teams from 13 countries in the Asia Pacific region. Cf. www.apcert.org/

79. www.govcert.nl

80. European Governmental CERTs (including GOVCERT.NL, and the CERTs of France, Germany, Finland, Sweden and the United Kingdom).

81. The Forum of Incident Response and Security Teams.

In **Norway**, a *National CERT* has been established at the National Security Authority (NSA) where it will be integrated with the already existing "*Detection and Alert System for Digital Infrastructure*" (VDI). The combined unit is oriented towards protection of critical infrastructures. In addition the *Center for Information Security* (SIS) has been relocated to the University of Gjøvik where it is embedded in a network of businesses and public institutions. The Center for Information Security will serve SMEs in the private and public sectors and the general society in a preventive mode of operation distributing information and knowledge. The National CERT and the Center for Information Security are co-financed by the Government and private companies. The *Norwegian Post and Telecommunication Authority* (NPT) has responsibility for security and preparedness in public networks, which includes to: (*i*) define and enforce security and preparedness requirements in public ICT network; (*ii*) consider investments in elements which can improve network robustness; (*iii*) verify that security requirements are implemented as specified; (*iv*) contribute to increased awareness and competence among Service Providers, Network operators and others; and (*v*) arrange exercises and contribute to co-operation between telecom operators.

In the **Slovak Republic**, there is currently no computer security incident response team (CSIRT), but activities are underway to establish such an institution in the near future (2005-2006).

The **Spanish** *Early Alert Center* for virus and information security (http://alerta-antivirus.red.es) is a service provided for Red.es,[85] an agency in the Telecommunications and Information Society State Secretariat in the Ministry of Industry, Tourism and Commerce, where all Internet users can obtain free and detailed information about viruses, and on actual and past alerts. Furthermore, there are other Alert and Response Centres: The *Cataluña Politechnic University Antivirus Alert Centre*, esCERT – UPC (Security Unit for emergency co-ordination in networks), established in 1994, provides assistance and assessment on information security and network incidents management. The security service in *RedIris* (IRIS-CERT) has the objective to detect problems affecting the network security in the RedIris centres,[86] and to take co-ordinated action as appropriate. They provide for prevention, warning on potential problems in due time, and are offering assessment to the different centres, and other complementary services, including the organisation of events.

In **Sweden**, legislation was changed in 2004 to make information about computer incidents classified, so that they would not fall under freedom of information acts. The aim was to increase willingness to report incidents to the Swedish IT Incident Centre (Sitic).[87]

In the **United Kingdom**, the *National Infrastructure Security Co-ordination Centre* (NISCC[88]) was established in 1999 to co-ordinate national efforts to protect the Critical National Infrastructure from electronic attack. As part of this role, NISCC oversees Uniras, the UK Government's Computer

82. The Trans-European Research and Education Networks Association.

83. The International Information Integrity Institute, an international partnership for ICT security with members from industry and private sector.

84. SURFnet-CERT is the CERT of the main Internet provider of higher education institutes and of many research organisations in the Netherlands. It was founded in 1992 and handles all computer security incidents in which a SURFnet customer is involved. The activities of SURFnet-CERT include education, expertise and knowledge dissemination, early warning, research and coordination of security incidents. www.cert.nl

85. www.red.es

86. Cf. http://rediris.es/cert.

87. www.sitic.se

88. www.niscc.gov.uk

Emergency Response Team (CERT). NISCC also acts as a focal point for information sharing between other public and private sector CERTS within the UK and plays an active part in the European (TF-CSIRT) and global CERT networks (FIRST). NISCC has also developed a different approach to incident watch and warning called WARPS (*Warning Advice and Reporting Points*[89]). The role of the WARPs is to provide highly relevant, customised, real-time advice to defined user communities — particularly communities which could not support an own CERT capability. Furthermore, the UK has developed a simpler national alerting service on major IT security threats — *ITsafe*[90] — aimed at non-technical home users and micro-businesses.

From the **United States**, the following initiatives were reported:

- The *National Cyber Security Division* (NCSD[91]), created in June 2003, is the national focal point for addressing cyber security and co-ordinating implementation of the National Strategy to Secure Cyberspace.[92] NCSD has created the *US Computer Emergency Readiness Team* (US-CERT) – a partnership between NCSD and the public and private sectors that is the operational arm of NCSD's cyber analysis and incident response activity.[93]

89. WARPs work to a code of conduct developed by NISCC. NISCC assist the setting up of WARPs by providing free of charge a toolbox and some software that was developed with help from the private sector (cf. www.warp.gov.uk). The WARP concept has attracted a lot of international interest and it is likely that the developing network of WARPs will extend beyond the UK.

90. www.itsafe.gov.uk. The Web site provides basic, plain language guidance on information security issues. ITsafe alerts are available in the form of e-mail or SMS.

91. NCSD is a division of the Office of Infrastructure Protection (IP) in the Information Analysis and Infrastructure Protection (IAIP) Directorate of the Department of Homeland Security.

92. NCSD is organised in four branches: (*i*) The Operations Branch facilitates collaboration and information sharing amongst government agencies and between government and the private sector and runs the US Computer Emergency Readiness Center (US-CERT), a 24x7 operations centre for cyber watch, warning, and incident response; (*ii*) The Law Enforcement and Intelligence Branch shares and coordinates cyber security information across government jurisdictions, and manages the National Cyber Response Coordination Group (NCRCG); (*iii*) The Awareness and Outreach Branch focuses on raising cyber security awareness levels and disseminating timely and actionable information to the public, private sector, and international stakeholders; and (*iv*) The Strategic Initiatives Branch works on cyber security for the long term, including critical infrastructure protection for cyber security, control systems, software assurance, training and education, exercise planning and co-ordination, standards and best practices, and cyber research and development co-ordination. Cf. http://csrc.nist.gov/sec-cert/index.html.

93. Within US-CERT, NCSD has established several important components: The US-CERT Operations Center serves as a real-time focal point for cyber security, conducting daily conference calls with US-based watch and warning centres to share classified and unclassified security information. The Homeland Security Information Network (HSIN)/US-CERT Portal provides a secure Web-based collaborative system to share sensitive cyber-related information with government and industry members. The US-CERT Control Systems Center serves as an operational and strategic component of the US-CERT's capability for addressing security issues in control systems. US-CERT co-ordinates its findings and follow-on actions with other divisions of IP, especially ICD and PSD. The US-CERT Public Web site provides government, private sector, and the public with information needed to improve their ability to protect their information systems and infrastructures. The National Cyber Response Coordination Group (NCRCG) is composed of officials from federal agencies and the private sector. It co-ordinates public-private cyber preparedness and incident response. The National Cyber Alert System (NCAS) delivers targeted, timely, and actionable information to the public to allow them to secure their computer systems.

- *EINSTEIN* is a program designed to build cyber-related situational awareness (currently in pilot phase). It facilitates the sharing of traffic data from federal government agencies' Internet access gateways and analyses the associated traffic patterns and behaviour.

- The US-CERT *Malicious Code Lab* analyses computer software to detect weaknesses with regard to malicious code and develops counter measures.

- The Department of Homeland Security (DHS) has established a *National Exercise Program Office* to co-ordinate exercises designed to assess preparedness and processes in the event of an attack on the nation including cyber and CIIP related attacks.

- The *National Communications System* (NCS), another agency of the DHS, periodically meets with international partners to share information on best practices for establishing and managing effective industry and Government partnerships. It co-ordinates with the National Cyber Security Division (NCSD) of DHS to respond to international queries specific to cyber issues.[94]

- Within the NCS, the *National Co-ordinating Center for Telecommunications (NCC) Information Sharing and Analysis Center (ISAC)* operates a 24x7 watch, which manages the entire Telecom ISAC information sharing process and provides the central analysis function for the ISAC. Information shared includes vulnerabilities, threats, intrusions, anomalies, and mitigation responses. The NCC Telecom ISAC includes representatives from industry and government.

- The *National Institute of Standards and Technology* (NIST[95]), has in January 2004 published the *Computer Security Incident Handling Guide*,[96] which provides guidelines for incident handling, particularly for analysing incident-related data and determining the appropriate response to each incident, that can be followed independently of particular hardware platforms, operating systems, protocols, or applications.

c) Critical infrastructure

In November 2002, the **Australian** Government endorsed the recommendations of the Business-Government Task Force on Critical Infrastructure, which included *inter alia* the establishment of a trusted information sharing network overseen by an advisory council. The *Australian Trusted Information Sharing Network* (TISN)[97] was launched by the government in April 2003, to enable owners and operators of the national critical infrastructure to share information and develop strategies to mitigate risk to critical infrastructure. TISN comprises the Critical Infrastructure Advisory Council (CIAC), a number of

94. www.ncs.gov/ncc/

95. The National Institute of Standards and Technology (NIST), is leading the development of information system security standards and guidelines, including security categorisation standards, as well as standards and guidelines for the specification, selection, and testing of security controls for information systems. NIST also: (*i*) conducts research, on information security vulnerabilities, and on techniques for providing cost-effective information security; (*ii*) develops performance indicators and measures for Federal Agency information security policies and practices; (*iii*) evaluates private sector information security policies and practices and commercially available IT technologies to assess potential application by agencies, and (*iv*) assist the private sector, upon request, in using and applying the results of research and standards/guidelines.

96. NIST Special Publication 800-61.

97. www.tisn.gov.au

Infrastructure Assurance Advisory Groups (IAAGs)[98] and a number of Expert Advisory Groups (EAGs).[99] The TISN works closely with the National Counter-Terrorism Committee (NCTC), Emergency Management Australia and other government and private sector organisations to ensure the co-ordination of the wide range of existing strategies, plans and procedures already existing to deal with the prevention, preparedness, response and recovery arrangements for disasters and emergencies. TISN members receive information about international best practices through e-mail, meetings and the TISN Web site. State and local governments are represented on the peak TISN body, and attend meetings of critical infrastructure sector groups.

The *Critical Infrastructure Advisory Council* (CIAC) is currently considering a draft National Strategy for CIP, developed by the Attorney-General's Department, which provides an overarching statement of principles, strategies and responsibilities for CIP in Australia from an 'all hazards' perspective. The strategy recognises the relationship between CIP and a significant number of strategies, plans and procedures already existing to deal with the prevention, preparedness, response and recovery arrangements for disasters and emergencies. The strategy is being prepared in consultation with the CIAC and builds on the work of the National Counter-Terrorism Committee.

The **Austrian** government has two main projects to protect critical infrastructures: CIRCA[100] and the ZAS (*Zentrales Ausweich System*).[101] These projects are managed and overviewed centrally by the Chief Information officer and a nominated department.

In **Canada**, the "Public Safety and Emergency Preparedness Canada" (PSEPC) released in November 2004 a position paper on a national strategy for critical infrastructure protection.[102] The key components identified for a strategy in this paper are that: *i*) CI sectors and owners are aware of, accept and take action on the accountabilities, risks and vulnerabilities to their CI; *ii*) The Government of Canada has an ongoing program to assure its physical and cyber infrastructures and thereby demonstrates leadership to other sectors; and, *iii*) New knowledge and tools for CIP are developed and shared. At present, feedback on the position paper is sought from stakeholder groups. The strategy itself is also under development.

Governments in Canada use established risk management approaches for critical infrastructure protection. Assurance actions and the priorities of those actions are based on risk management principles that employ common criteria where appropriate. Critical infrastructure (CI) partners are encouraged to use a consistent set of criteria to identify and rank their CI, and to determine the relative level of risk. The Canadian National Critical Infrastructure Assurance Program (NCIAP) promotes a national partnership

98. The IAAGs for different critical infrastructure sectors comprise representatives from across the respective industry sectors including communications and energy.

99. The CIAC has set up two permanent EAGs in 2003, the Information Technology Security EAG and a CIP Futures EAG.

100. Cf. question 2a) above. One of the topics currently discussed in CIRCA is Critical Information Infrastructure Protection.

101. In 1980, the Federal Chancellery established a data centre in a sub-terranean high-security area to host the Austrian government's central backup system for communication and IT (*Zentrales Ausweich System* – ZAS). Some government IT-applications are running on that site, for other government IT-systems there is a backup solution in case the main systems in Vienna are unavailable for crisis reasons, or maintenance work. ZAS is also the main data centre for the State Crisis Management of Austria.

102. Canada defines its national critical infrastructure (NCI) as "those physical and information technology facilities, networks, services and assets, which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada".

among private and public sector stakeholders. The Government fosters co-operation and communication across sectors, as most of the countries' infrastructure is privately owned. A component of the NCIAP addresses cross-border systems and networks, including the Internet, banking networks, gas and oil pipelines.

The **Czech Republic** has set up an information portal on crisis management.[103]

The **Finnish** *Government Information Security Management Board* has published instructions on critical infrastructure, for example a public information security instruction for critical ICT systems.

In **France**, studies conducted on national protection and security have highlighted the crucial role of critical infrastructure. The components of this infrastructure are interdependent. Their operation hinges in many cases on information and communication systems. The main sectors identified are electric power, telecommunications, transport, the chain of inter-bank transactions, the health watch network, the social benefit chain and the distribution of drinking water. The work carried out to ensure better protection for critical infrastructure in France does not dissociate "physical infrastructure" aspects from "information systems" aspects. A revision of the legal framework on critical infrastructure is expected. A draft decree on the subject is being prepared.

In **Germany**, organisations in the Federal Ministry of the Interior responsible for protecting critical infrastructures (KRITIS) at federal level are the Federal Office for Information Security (BSI), the German Federal Criminal Police Office (BKA), the newly established Federal Office for Civil Protection and Disaster Response (BBK), the Federal Border Police (BGS) and, from other ministries, the Regulatory Authority for Telecommunications and Posts (RegTP), the Federal Railway Authority, the Federal Office for Radiation Protection and the Federal Armed Forces. The work of the different federal authorities is co-ordinated through the "KRITIS working group" (AK KRITIS)[104] at the Federal Ministry of Interior.

A system of permanent co-operation was instituted between the specialist agencies of the Federal Office for Civil Protection and Disaster Response (BBK), the Federal Agency for Technical Aid (THW), the Federal Office for Information Security and the Federal Criminal Police Office in order to provide operative support for the working group at the Federal Ministry of the Interior. Consultations have been held according to priorities identified by the working group, initially with the ministries concerned, and other relevant organisations (associations, industry). Process-orientated studies of the situation of IT-dependent critical infrastructures had been prepared by the Federal Office for Information Security already in late 2002, in close co-operation with the owners and operators of critical infrastructures.

In **Japan**, the *IT Security Promotion Committee* adopted a *Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure* (December 2000). Based on this plan, public and private sectors have taken measures to protect Critical Infrastructures.[105]

Based on the "e-Japan strategy II Acceleration Program Package", in order to protect the information systems of critical infrastructure from disaster and cyber-attacks, the *IT security office of the Cabinet Secretariat* is now deliberating on the minimum technical and operational standards to be met by information systems, in co-operation with ministries and agencies related to information security.

---

103. www.krizove-rizeni.cz/ (available only in the Czech language).

104. The working group's mission is to generally enhance the level of protection for critical infrastructures in order to reduce the country's vulnerability, by developing protection concepts designed to result in the implementation of concrete actions, in co-operation with owners and operators of critical infrastructures.

105. Cf. www.bits.go.jp/en/sisaku/cyber_terror.html.

A *Committee for Essential IT Security Issues* was established in 2004, and since December 2004 the Cabinet Secretariat and relevant ministries and agencies have been working to lay out the measures required of both the government and private sectors to assure IT security in Critical Infrastructures, with participation of representatives from infrastructure sectors on the respective subcommittee.

The Ministry for Economy, Trade and Industry (METI), the Information-technology Promotion Agency (IPA) and JPCERT/CC[106] maintain an application for *Computer Virus / Unauthorized Computer Access Incident Reports*, operate a *Traffic Monitoring system* on the Internet, and a *Vulnerability Handling Framework*. METI also provides *cyber exercises* for information systems of e-commerce companies.

As a proactive measure against cyber-terrorism, to prevent the expansion of damage and facilitate the arresting of cyber-terrorism suspects or criminals, the National Police Agency (NPA) continues to strengthen co-operation with the private sector, by visiting critical information infrastructure operators to ask for improvement of security measures, prompt notice to the police and co-operation in investigations, to provide information about vulnerability of computer programs and computer viruses, to raise awareness for, and advise on measures against cyber-terrorism.

In 2001, the **Korean** Government established the *Information Infrastructure Protection Act* and performed an analysis and evaluation of the vulnerabilities of the infrastructure facilities that are considered to be critical to national security. In the same year, the government established the *Committee on the Protection of Information Infrastructure*, which consists of the ministers from all ministries, and is chaired by the prime minister. The committee discusses the selection of the critical infrastructure facilities and the principal policies related to improving the relevant systems.

In the **Netherlands**, the Ministry of the Interior and Kingdom Relations launched an interdepartmental project entitled *Protection of the Dutch Critical Infrastructure* in 2002. The list of critical sectors, products and services in the Netherlands includes 11 sectors, among them Telecommunication/ICT. The protection of the Telecommunication/ICT infrastructure has been defined in the project *Vital Infrastructure Telecommunications/ICT (VISTIC)*. The Ministry of Economic Affairs is primarily responsible for the execution of the VISTIC project, which is being conducted in close collaboration with other (inter-)national government agencies, and telecommunication operators, consumers and experts.[107] The objectives of the VISTIC project include the determination of critical elements in the telecommunications/ICT infrastructure, performing risk-analysis, and making recommendations on the implementation of measures to reduce the vulnerability of telecommunications/ICT infrastructure. VISTIC is planned to end in December 2005.

A NAtional COntinuityplan TELecommunication (*NAtionaal COntinuïteitsplan TELecommunicatie - NACOTEL*) was established in June 2001 with the objective of formulating a contingency policy and a programme for crisis management in the telecommunications sector. NACOTEL recommends organising the sector in a way that ideally avoids, but also promptly rectifies serious disruptions to the system that

106. The Japan Computer Emergency Response Team Coordination Center.

107. The first phase in this intergovernmental project is to obtain an overview of the critical products and services and their (inter-)dependencies, and a preliminary view of potential damage as a result of failures of any one of these products and services. Phase two involves a full inventory of contingency and protection measures already in place, recommendations for the promotion of best practice, and the preparation of a risk and/or vulnerability analysis of each critical sector. Phase three of the project will involve in-depth assessment of improvements that need to be made immediately to increase the reliability of the critical infrastructure, and how this infrastructure could be further enhanced.

would damage vital sectors of society.[108] The project is a public-private partnership (PPP) between the Ministry and seven telecom providers,[109] which were requested to join the partnership, as they already had an obligation under the Telecommunications Act to have contingency plans in place in case of a national crisis.[110] Two other parties in the PPP were a process facilitator (for building confidence, neutrality) and a consultant (auditing of implemented agreement).

In June 2001 the participants to the PPP signed an agreement for two years with regard to: *a*) how telecommunication services can continue uninterrupted; and *b*) how a fault can be rectified as quickly as possible. This includes the preparation of a contingency plan and of a report on the production of the contingency plan, establishing a crisis management plan, and regularly producing incident reports for major incidents. After the two-year agreement ended, actions were taken to develop a new framework to continue and improve the work done in those two years. These actions include increasing the number of participating providers and the creation of a basis in legislation for NACOTEL, which would facilitate greater co-operation between the participating organisations and further clarify responsibilities. An agreement has been reached on the implementation and use of results: the contingency plan format, periodic reporting on contingency planning, incident reporting, reviewing of incidents.

Some of the obstacles to full collaboration and transparency in NACOTEL are: *i*) Tension between commercial interests and public responsibility within the providers organisation; *ii*) Trust: these providers operate in a highly competitive market, and here they have to work together; and *iii*) Capacity for participating in NACOTEL: due to the Public Private Partnership (PPP), versus *e.g.* legislation, it is difficult to find sufficient consensus on all subjects to keep the participants "around the table".[111]

The *National High-Tech Crime Center* (NHTCC) is currently engaged in a project at Schiphol Airport to make an inventory of the critical infrastructures and to get an insight into the division of responsibility.

In **Norway**, the Ministry of Justice has established a high-level national infrastructure committee (*infrastrukturutvalget*) which will *i*) conduct a survey of the measures and actions used to maintain national security when public bodies are made private; *ii*) identify operations with vital importance for the national security; and *iii*) conduct a survey of the measures and actions used to maintain national security in relation to private operations or operations partly owned by the state. The *Norwegian National Security Authority* (NSA) administrates the *Detection and Alert System for Digital Infrastructure* (VDI), a co-operation between NSA, the police, and participants from industry. VDI identifies attacks in the networks, and issues alerts to partners in the VDI-system. One of NPTs main responsibilities is to analyse the critical information infrastructure in order to identify vulnerabilities. A follow-up of this activity will be to propose overall requirements to the critical information infrastructure. Furthermore, the *Norwegian Defence*

108. Most of the largest national telecom providers – KPN Mobile, Vodafone, Telfort, Orange, T-Mobile (mobile telecom providers) and KPN, BT and Enertel (fixed telecom providers) – and the Directorate-General of Telecommunications and Post (DGTP) of the Ministry of Economic Affairs have agreed arrangements on how to fulfil this objective.

109. The responsibilities of the telecom providers participating in NACOTEL are: *i*) Improving agreements on contingency planning and crisis management (involving all participants); *ii*) Dialogue and co-operation (involving all participants); and *iii*) Implementing agreements and acting accordingly.

110. In cases of large security risks and national crises the Minister is authorised under article 14.1-14.6. of the telecommunications law (TW) to determine how the functioning of the telecommunication infrastructure and the use shall be guaranteed.

111. www.minez.nl/content.jsp?objectid=31278c

Research Establishment (NDRE) is conducting a *research project* on Critical Information Infrastructure Protection.[112]

Spain has established basic regulations on critical infrastructure by defining the following objectives in the *Telecommunications General Law* (November 2003): *i*) to maintain a high degree of protection of privacy and personal data; *ii*) To guarantee the integrity and security in public telecommunications networks; and *iii*) to allow for the setting of conditions, in addition to general authorisations, with regard to the security of networks and information; *iv*) to guarantee the availability and integrity of public fixed telephone networks. In addition, operators providing fixed telephones services, in locations, must take all measures to guarantee permanent access to emergency services. Finally, *v*) an obligation is imposed on operators to adopt technical and organisational measures to monitor the security of services, and to guarantee the confidentiality of communications and of related traffic data.

Also in this context, the Ministry of Industry, Tourism, and Commerce, has created a legal framework for digital signatures. The *Digital Signature Law* of December 2003 (59/2003) also includes provisions for a Digital National Identity card. It is aimed at fostering the use of digital signature in Spain, to increase citizens' confidence in telematic services**.**

In **Sweden**, actors in the area of technical infrastructure collaborate on an operational level, and initiatives such as the Swedish IT Incident Centre supply critical infrastructure organisations with information and a decision basis. These activities are co-ordinated by the Swedish Emergency Management Agency (SEMA).

In the **United Kingdom**, the *National Infrastructure Security Co-ordination Centre* (NISCC[113]) was established in 1999 to co-ordinate national efforts to protect the Critical National Infrastructure from electronic attack. NISCC is a cross departmental centre which brings together a number of government organisations and works closely with private sector and public sector partners. The principal activities of NISCC are assessing the threat from electronic attack; response, including the CERT work described above under 2b); research and development, and outreach to private and public sector organisations in the critical business sectors. It engages with the management of the key infrastructure providers in the United Kingdom on the security of their IT systems and the resilience of their communications. In addition, NISCC promotes information sharing at several levels and has developed an information exchange model in addition to the WARPs (Warning Advice and Reporting Points).[114] It acts as a centre of excellence in questions of technology vulnerability and the managed disclosure and remediation of those vulnerabilities, and promotes information sharing in key communities such as the financial or the communications sector.

In the **United States**, the Homeland Security Act of 2002 renewed the country's focus on critical infrastructure protection. Subsequent national strategies — The *National Strategy for Homeland Security*, The *National Strategy for the Physical Protection of Critical Infrastructures*, and The *National Strategy to Secure Cyberspace* — provide specific strategies for how the Government in partnership with critical infrastructure owners and operators, the private sector, and individual citizens can enhance the Nation's security. The *National Strategy for the Physical Protection of Critical Infrastructures* emphasises the new paradigm of co-operation and partnership, which is necessary since an estimated 85% of critical infrastructures in the United States are privately owned. The *Department of Homeland Security* (DHS) is charged with protecting the people and critical infrastructures of the United States.

112. The "BAS5" project; cf. Question 11 below.

113. www.niscc.gov.uk

114. Cf. question 2b) above.

As part of the Critical Infrastructure Protection initiative mandated under Homeland Security Presidential Directive 7 (HSPD-7) of 17 December 2003, DHS also co-ordinates vulnerability assessments of *critical infrastructures* in co-operation with the designated sector-specific agencies. Under HSPD-7, DHS is the lead agency to develop a national plan to protect the nation's critical infrastructures. HSPD-7 identifies 17 sectors and the associated sector-specific agencies that for their sector have responsibility to identify critical assets, develop methodologies to assess vulnerabilities, and map those vulnerabilities to critical assets in a risk assessment analysis. DHS is responsible for the overarching correlation, analysis, and trending of the information provided by those agencies. DHS is also responsible for performing the overarching risk analysis which will weigh cyber risks along side physical risks in determining the overall risk ranking of each asset within and across infrastructure sectors.

DHS is also the *information technology (IT) sector-specific agency*, and NCSD has been delegated the sector-specific responsibility for the IT Sector. NCSD is charged with identifying the critical assets and related vulnerabilities within the IT sector. Additionally, NCSD is producing a comprehensive inventory of cyber security assessment, remediation, and mitigation activities conducted within and across critical infrastructure sectors.

DHS's *Information Analysis and Infrastructure Protection (IAIP) Directorate* has the mission of identifying and assessing current and future threats to the homeland, map those threats against existing vulnerabilities, issue timely warnings and take preventive and protective action. It takes a holistic view of critical infrastructure vulnerabilities and works to protect the country from all threats by ensuring the integration of physical and cyber security concerns. IAIP considers the full range of risks to the nation, including loss of life, disruptions of infrastructure services, economic impact, and national security implications. The IAIP Directorate's Infrastructure Protection Branch (IP) includes the NCS, the National Cyber Security Division (NCSD), the Infrastructure Co-ordination Division (ICD),[115] and the Protective Security Division.

The Homeland Security Presidential Directive 7 (HSPD-7), requires the development of a national plan to protect the nation's infrastructure.[116] The *National Response Plan*, released in January 2005, establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. The Plan incorporates best practices and procedures from incident management disciplines — homeland security, emergency management, law enforcement, fire fighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector — and integrates them into a unified structure. The *National Communications System* (NCS) is the lead for incidents involving communications and NCSD is the lead for cyber incidents. The plan includes annexes that summarise the roles and responsibilities of different organisations when responding to different types of incidents.

The Homeland Security Act of 2002 included a section known as the Critical Infrastructure Information Act of 2002 (CII Act), which provides for the protection of voluntarily shared critical infrastructure information (CII). The CII Act defined CII as, "information not customarily in the public domain and related to the security of critical infrastructure or protected systems."[117] There are no

115. The Infrastructure Coordination Division (ICD) was created in July 2003 as a national focal point for interfacing with the nation's critical infrastructures and for facilitating the implementation of the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.

116. Cf. www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

117. Protected CII (PCII) voluntarily submitted according to PCII Program procedures, is exempt from disclosure under the Freedom of Information Act (FOIA), as a result of pressure from industry to protect proprietary information voluntarily submitted to Government.

regulations that mandate critical infrastructure owners and operators to submit information about their assets to the Federal Government.

The White House *Office of Science and Technology Policy* (OSTP) established a *Critical Information Infrastructure Protection Interagency Working Group* (CIIP IWG) under the National Science and Technology Council. The Director of Cyber Security R&D in the DHS S&T Directorate co-chairs this interagency working group, which includes participation from 20 organisations in 11 departments and agencies, as well as from several offices in the White House. The CIIP IWG currently is engaged in regular meetings aimed at developing R&D plans in response to the US National Cyber Security Strategy and the Presidential Directive HSPD-7.

d) Risk assessment

In **Austria**, risk assessment is, for example, part of the supervision and accreditation of certification service providers (CSPs).[118] If a CSP claims to fulfil additional standards (like BS 7799 or ETSI TS 101 456), the supervisory authority also checks for compliance with these standards.

Governments in **Canada** use established risk management approaches to fulfil their responsibilities for critical infrastructure protection to Canadians. On this basis, assurance actions and the priorities of those actions are based on risk management principles that employ common criteria where appropriate. Critical infrastructure (CI) partners are encouraged to use a consistent set of criteria to identify and rank their CI, and to determine the relative level of risk. The relative criticality and priority of CI assets are identified by assessing the impact of their loss on the operation of the sector (and other sectors) and the consequences of their loss. Owners and operators make decisions about safeguarding and assuring their own CI assets.[119] Another key element of risk management is information sharing: The more information available to organisations about potential threats and vulnerabilities, the better they will be able to understand the risk and ensure the continuity of essential services.[120] To this end, new governance mechanisms, information integration centres and modernising legislation are being studied.

In **Finland**, the Government Information Security Management Board (VAHTI) and the Ministry of Finance have implemented several inter-governmental projects to strengthen risk assessment work in ministries and agencies, using specific government instructions for information security risk assessment prepared by VAHTI.

---

118. For providers of qualified certificates, the supervisory authority for electronic signatures has to examine *i*) the reliability of CSPs, *ii*) the availability of directory and revocation services, *iii*) the quality of timestamps, *iv*) knowledge, the experience, and the qualifications of the CSPs' personnel, *v*) financial resources of CSPs, *vi*) the documentation of the life cycles of certificates, and *vii*) fulfilment of technical requirements (*e.g.* use of trustworthy systems). Risk assessment in this context is primarily based on the requirements of the Signature Act and the Signature Decree. According to the Signature Decree, any CSP has to notify the supervisory authority of specific threats and risks relevant to the security of certification services.

119. In general, the components of the risk management for CI include: *i*) understanding and creating an awareness of CI and its interdependencies; *ii*) assuring CI through threat and vulnerability assessments, mitigation and preparation, research and development; and *iii*) managing response and recovery through facilitating cross-sector co-ordination, response planning and education.

120. Information that needs to be shared includes information about threats, vulnerabilities, incidents, protection, mitigation measures, best practices etc. On this basis, information sharing can be viewed as a means to better manage risk, and in turn, help deter, prevent, mitigate and respond to threats.

In **France**, a draft ordinance under preparation will require central and local public authorities that institute remote services or information systems for communicating with other government authorities to take information system security issues into consideration and, in particular, to conduct a risk analysis.

The *Central Directorate for Information Systems Security* (DCSSI) has developed an information system security risk assessment and management methodology – the EBIOS standard ("Expression of Needs and Identification of Security Objectives"). This methodology has been widely disseminated and used in the public and private sectors, and training on the subject is dispensed by the DSCCI training centre. It also contributes to: *i*) Risk management, and risk re-assessment, as included in the OECD 2002 *Security Guidelines*; and *ii*) Exploration of the ongoing process of information system security risk management.[121]

The DCSSI has also set up an "EBIOS Club" to sustain and improve the method and how it is applied. The initiative seeks to:

- Share information on EBIOS implementation between the public and private sectors.
- Improve the EBIOS approach by identifying best practices, developing software to implement the technology that is available to all free of charge (1 300 CDs distributed) and contributing to training (70 persons per year) and communication activities.
- Standardise practices and tools for the public and private sectors.
- Develop an individual qualification label acknowledging know-how in this area.
- Work on additional issues involving risk management (return on investment in security, certification of consultants, continuity of activities, etc.).

The "EBIOS Club" was created in 2003 on a voluntary basis and is run by the DCSSI advisory staff. It is made up of approximately 50 persons from the public and private sectors in France and other countries, and it meets regularly (six times per year). The Club has also set up working groups to tackle risk management issues, and it encourages all participants to exchange information throughout the year. The target groups are organisations that use EBIOS as consultants or customers in the public and private sectors in France and abroad, and aimed at promoting: *i*) the development of a culture of security and good practices in the realm of corporate strategies for information system security; and *ii*) De-facto standardisation.[122] The "EBIOS Club" initiative is considered a very good practice for exchanging information on risk analysis between the public and private sectors, and for co-operation with other national bodies. The initiative is considered as a good example for meeting the OECD's objectives for developing a culture of security in compliance with international standards.

In **Japan**, *Guidelines for IT Security Policy*, the IT Security office of the Cabinet Secretariat evaluated the implementation level of IT security policy of the ministries and agencies in 2002. In 2004 and 2005, the IT Security Office in the Cabinet Secretariat conducted vulnerability tests for the information systems of the governmental ministries and agencies in co-operation with the National Police Agency, and the

121. Documents on EBIOS are available on the DCSSI Web site at www.ssi.gouv.fr/en/confidence/methods.html (English); and www.ssi.gouv.fr/fr/confiance/ebios.html (French).

122. All the French Ministries use EBIOS to analyse the security risks of their information systems. An additional 100 EBIOS studies will be carried out in 2005 on new e-government services.

Defence Agency.[123] Information Security Auditing Standards were established by the Ministry for Economy, Trade and Industry (METI) in April 2003.

The **Korean** Government has been operating an evaluation and certification system in accordance with the *Act on Informatisation Promotion* since 1998 to provide for information security systems that are proven to be safe and reliable. Since 2005, the Ministry of Information and Communication (MIC) has been testing information security systems according to the "common criteria," which replaced the previously used "K-criteria." In addition, all information security systems used at public organisations are required to pass tests conducted by the National Security Research Institute and have to be approved by the Director of the National Intelligence Service.

The health sector in **Norway** has, together with the Directorate for Health and Social Affairs, developed a norm for Information Security in the health sector. The norm will set the level of information security for all those who exchange patient data. Additional guidelines will set out how the requirements may be met. The norm will be in effect from the second half of 2005. Norwegian hospitals have already now established regional information security policies and are co-ordinating these policies nationwide.

The **Spanish** "*Centro Criptológico Nacional*", a subordinate body of the "*Centro Nacional de Inteligencia*" has several competences with regard to risk assessment.[124] The *Public Administration Ministry* has developed the risk evaluation system MAGERIT.[125]

In Sweden, the Government regulation on crisis management in peace time states that all public authorities are to make a yearly assessment of risks and vulnerabilities in their area of responsibility. Some public agencies are responsible for takingactions on identified risks and vulnerabilities within their sector of responsibility. There are also rules concerning public agencies' risk management for government-internal insurance purposes.

In the **United Kingdom**, there is no discrete legal or regulatory basis for risk assessment in relation to Information Security, while many larger UK companies with operations in the United States are impacted by the US Sarbanes-Oxley Act, which has had a discernible effect on how these companies deal with information risk within their corporate structures. For information risk management, the predominant trend in the United Kingdom is the use of the ISO 17799 standard — the Guideline on Information Security Management[126] — and BS 7799 Part 2, a specification for an information security management system.[127]

ISO 17799 is widely used by the private sector and the Government's core internal security advice is based on it. The use of third party assessment against BS 7799 Part 2 is constantly increasing and it is expected to significantly further increase if and when the standard forms the basis of a new ISO standard in late 2005. The use of the standards is supported by a wide range of bodies; the British Standards Institution[128] provides implementation guidance and training; the Department of Trade and Industry

123. Cf. www.bits.go.jp/en/sisaku/h1509imple.html

124. For the corresponding regulatory framework, cf. www.oc.ccn.cni.es/pdf/RD421-2004CentroCriptologicoNacional.pdf

125. Cf. www.csi.map.es/csi/pg5m20.htm

126. Cf. www.iso.org

127. Cf. www.bsi-global.com

128. Cf. www.bsi-global.com

promotes the use of the standard and supports a large User Group;[129] and many colleges and private sector security and training consultants also provide related guidance and training.[130]

The **United States** reported the following activities with regard to risk assessment:

- The *National Communication System* (NCS) administers industry and government National Security Information Exchanges (NSIE) to discuss and share information related to network security issues. The NCS, in co-ordination with the President's National Security Telecommunications Advisory Committee (NSTAC),[131] established the NSIEs in 1991 as a structure for fostering an informal, collegial exchange on network security issues regarding the public switched telecommunications network (PSTN). The NSIEs periodically conduct risk assessments of the PSTN with regard to electronic intrusion. In recent years, the NSIEs began reaching out to Canada and the United Kingdom, who have representatives who participate in the NSIE meetings.

- In addition to the implementation of the national plan to protect the nation's critical infrastructures, the NCS Operational Analysis Branch regularly performs risk assessments for specific national security special events (*e.g.* national political conventions) and impending national disasters (*e.g.* hurricanes, volcanoes).

The *Federal Information Security Management Act* of 2002 (FISMA)[132] and the US Office of Management and Budget (OMB) security policies[133] require security assessments, and a continuing cycle of risk assessment for all Federal agencies. As a key component in the *E-Government Act of 2002,*[134] FISMA provides a framework for enhancing the effectiveness of information security in the federal government. The law re-affirms and expands the original responsibilities for computer security issues within the Federal Government in the *Computer Security Act of 1987.*[135] The National Institute for Standards and Technology (NIST) is leading the development of key information system security standards and guidelines to include the development of security categorisation standards, as well as standards and guidelines for the specification, selection, and testing of security controls for information systems.[136]

129. Cf. www.dti.gov.uk/bestpractice/assets/security/iso-group.pdf

130. Cf. for example www.xisec.com, which also contains a wealth of information on 7799 certification.

131. NSTAC is a Federal advisory committee comprising up to 30 senior executives from telecommunications service providers, software and hardware manufacturers, information and systems security providers, major information users, the aerospace industry, and trade associations. The NSTAC, established by Executive Order 12382 in 1982, provides industry-based advice and expertise on issues related to the implementation of NS/EP communication policy. Through its working body, the Industry Executive Subcommittee, the NSTAC studies topics related to infrastructure protection, including vulnerability analyses, protective methods, technological convergence, and infrastructure interdependencies. Studies and recommendations that are approved by the NSTAC are forwarded to the President for his consideration. https://www.ncs.gov/nstac/nstac.html

132. Public Law 107-347, Title III.

133. OMB Circular No. A-130, Appendix III, Security of Federal Automated Information Resources.

134. Public Law 107-347.

135. Public Law 100-235.

136. Cf. csrc.nist.gov/sec-cert/index.html.

e) Outreach to business, civil society and others

The **Australian** *High Tech Crime Centre* (AHTCC) engages with private sector organisations to build a private/public partnership to combating high tech crime. This has included secondments to the AHTCC from private sector organisations to conduct investigations, share intelligence and build capacity. The *Trusted Information Sharing Network* (TISN) works closely with the National Counter-Terrorism Committee (NCTC), Emergency Management Australia and other government and private sector organisations to ensure the co-ordination of the wide range of existing strategies, plans and procedures already existing to deal with the prevention, preparedness, response and recovery arrangements for disasters and emergencies.

In **Austria**, IT-security beyond legally required measures between private parties is mostly regulated by contract. Since there is no obligation to report such contracts to the authorities, unless special circumstances prevail (such as data processor agreements that must be reported to the data protection commission in some cases) it is not possible to specify any private sector agreements. Some national universities' central IT services (*Zentrale Informatikdienste*) have IT-security regulations and/or security policies in place.[137] The *Data Protection Commission* (*Datenschutzkommission*),[138] as part of its legal responsibilities under the data protection law, acts as an advisory service for citizens and businesses, with regard to IT-security measures to be taken under data protection legislation.

Another key resource in this context is the Austrian Handbook of IT-security,[139] published by the Chief Information Office (CIO, in the Federal Chancellery).[140] This handbook discusses on the one hand the establishment of comprehensive IT-security processes within authorities, businesses, etc; on the other hand it lists concrete measures that have to be taken for achieving a higher level of IT-security. Additional relevant measures have been taken in Austria *e.g.* by the Austrian Secure Information Technology Centre (A-SIT[141]) and the IAIK,[142] and by banks[143] and ISPs.[144]

---

137. Cf. *e.g.* http://www2.uibk.ac.at/zid/security/index.html (IT-security policy of the university of Innsbruck); www.zid.tugraz.at/regeln (IT-policy of the technical university of Graz), www.univie.ac.at/ZID/passwort (password policy of the Viennese university), and http://zidWeb.boku.ac.at/?id=sec-pol-e (IT-security policy of the university of natural resources and applied life sciences in Vienna).

138. www.dsk.gv.at/

139. *Österreichisches IT-Sicherheitshandbuch*, Chief Information Office, ICT-Staff Unit, *Teil 1: IT-Sicherheitsmanagement* Version 2.2 November 2004 and *Teil 2: IT-Sicherheitsmaßnahmen* Version 2.2 November 2004, www.cio.gv.at/securenetworks/sihb/

140. Cf. www.cio.gv.at/securenetworks/sihb/

141. A-SIT (www.a-sit.at) is an association – *i.e.* a private legal entity – founded by the Austrian Ministry of Finance, the Austrian central bank, and the technical university of Graz, with the objective to consolidate and develop know-how in the field of IT-security for public authorities, businesses and civil society. A-SIT also performs audits of certification authorities operating in Austria, as laid down in article 3 para. 4 Directive 1999/93/EC, respectively section 18 para. 5 Austrian Digital Signature Act.

142. www.iaik.tu-graz.ac.at

143. Banks started to offer online payment transactions and general banking services very early. They soon discovered that the application of Internet banking could help them cut their personnel costs drastically. In the beginning, authentication via Internet was provided by a simple logging in combination with additional one-time transaction numbers (TANs), to be typed in for each transaction. Nowadays the financial institutes tend towards identification and authentication according to the E-Government Act, secured by means of digital signatures. Banks in Austria are very interested in promoting digital signatures, and are among the organisations that are hoped to help popularise digital signature technology among consumers.

The Austrian Regulatory Authority for Broadcasting and Telecommunications [*Rundfunk- und Telekom Regulierungs-GmbH* - RTR] has published a certification practice statement, giving detailed advice of how to operate a certification service.[145]

In **Canada**, the federal Government has also become a signatory to an agreement to participate in Microsoft's Security Co-operation Program (SCP), a global initiative launched by Microsoft. Through the SCP, Canada's CCIRC and Microsoft will collaborate in responding to computer security incidents and proactively seek to reduce the effects of cyber attacks. The SCP initiative reinforces the Department's commitment to collaborate with the private sector to enhance Canada's cyber defences, as outlined in the National Security Policy. At the same time, Canadian law enforcement agencies and the information technology sector have taken steps to publicise the need to prevent and combat computer-aided criminal activity. This has been in response to computer virus and denial of service attacks.

In Finland, the government online discussion forum[146] has been used for online discussions about information security. The database of projects in Ministries in Finland (HARE),[147] built by the Ministry of Finance, has been used to deliver information about public information security projects undertaken in all ministries. The database contains update information about significant projects, including information security projects, in the ministries.

The **French** Central Directorate for Information Systems Security (DCSSI) has the following activities specifically aimed at the business community:

The French *Centre for Information Technologies Security Certification*, a unit of the DCSSI, has responsibility for the information technology security certification scheme. In this capacity it:

- Licenses and supervises information technology security evaluation facilities.
- Supervises evaluations.
- Analyses evaluation reports.
- Issues certificates and certification reports.

The Centre reviews certifications in the light of directives laid down by the Certification Steering Committee. Certification is based on evaluations carried out by laboratories licensed by the Prime Minister, and approved by the French Accreditation Committee (COFRAC) in accordance with the NF EN ISO/CEI 17025 standard. Evaluations are carried out against standards or guidelines specified by the DCSSI using the Common Criteria (CC) or ITSEC methodology. Certificates issued by the DCSSI attest

144. The "Internet Service Providers Austria" (ISPA; www.ispa.at/), an association of ISPs, encourages its members to secure their networks. The have also agreed on a code of conduct for spam; cf. www.ispa.at/downloads/COC_spam_english.pdf (in English language).

145. Issues like liability, issuing and renewal of certificates, internal audits, privacy, identification and authentication, blocking and revocation of certificates, logging and archiving duties as well as physical, organisational and personal security measures are addressed in this book. www.signatur.rtr.at/repository/tkk-cps-12-20041220-de.pdf

146. www.otakantaa.fi

147. www.hare.vn.fi

that the certified products are compliant with a technical specification of the "security target". This security target may itself be certified as compliant with a specification package known as a "protection profile".[148]

This activity is focused both on the IT security industry, to which it affords an opportunity to certify the security offered by its products, and on the owners of information systems, in order to promote the use of trusted products whose security has been evaluated.[149] Certificates issued in France are recognised in other countries through two agreements for mutual recognition.[150]

State- industry workshops with the industry, organised by the DCSSI on issues involving the security of information systems and networks, seek to validate good practices in the realm of technical issues with players in the field of information system security from government and industry. Each workshop focuses on a technical topic formulated to address a concern or meet a need of industry and government. The workshops provide a forum for discussion of projects prepared by the DSCCI, and they encourage participants to share experiences, leading to "soft validation" of certain recommendations or the launch of some new area of exploration. They endeavour to promote good practices in the design of IT security systems and their implementation in industry.[151] One of the results of those workshops is the approval of some recommendations on cryptographic algorithms issued by DCSSI, and available to the public.[152]

In **Germany**, many activities to promote the trustworthiness of information and communication technologies are carried out in co-operation with TeleTrusT Deutschland e.V. (TTT).[153]

Japan has in March 2003 set up the *MIC Information Security Site for the People* in order to familiarize the general public with measures taken by the government on information security. In addition, tax support measures for companies and private operators buying network security enhancement equipment, or network security maintenance equipment, are being taken. Financial support based on

148. Protection profiles outline high-level requirements which may serve a variety of common interests such as in the banking community, the health care industry, in transport etc.

149. In 2003, the French body for IT security certification issued: 25 certificates for "smart cards"; 3 certificates for software; and 8 certificates for protection profiles.

150. The 1999 SOG-IS European Mutual Recognition Agreement provides for mutual recognition of certificates issued by the certification bodies of any signatory State. European mutual recognition extends up to the ITSEC E6 and CC EAL7 levels. The Common Criteria Mutual Recognition Arrangement (CC-MRA) provides for mutual recognition of certificates issued on the basis of common-criteria certification frameworks. Mutual recognition applies up to evaluation level EAL4 and to the ALC_FLR family. For further information about the French Centre for Information Technology Security Evaluation, cf. www.ssi.gouv.fr/en/confidence/evalcertif.html.

151. In 2003 and 2004, four workshops were organised by the DCSSI on the interconnection of IP networks, remote access, cryptographic algorithms, and authentication. An average of 40 people took part in each workshop. A number of technical documents were approved, to be used by all interested parties.

152. www.ssi.gouv.fr/site_documents/politiqueproduit/Mecanismes_cryptographique_v1_02_standard.pdf

153. TeleTrusT Deutschland e.V. was established in 1989 as an association dedicated to promoting the trustworthiness of applications and services based on electronic signatures, authentication and encryption in an open system environment. It comprises Working groups and task forces. Services offered include the "ISIS-MTT Application Centre" (ISIS-*MTTAnwendungszentrum*) and the "European Bridge-CA". TeleTrusT co-operates with institutions in other countries in order to harmonise goals and standards within the European Union, and has been chairing the program committee of the European conference for information security (Information Security Solutions Europe - ISSE) since 1999. TeleTrusT also represents Germany in the European Biometric Forum (EBF). Cf. www.teletrust.de

government's loan and investment programs for IT users and suppliers in order to promote their procurement of secure systems and products is also provided.

Furthermore, the Ministry for Economy, Trade and Industry (METI) holds nationwide seminars in collaboration with NPO on countermeasures against computer viruses and unauthorised access, intended for IT users in general. The Information-technology Promotion Agency (IPA) and JPCERT/CC[154] hold similar nationwide seminars for administrators of information systems. Finally, to initiate and promote close co-operation between the police and industries, the National Police Agency (NPA) has convened a *Comprehensive Security Meeting* for co-operation between government agencies, such as the police, and industrial circles. Each prefectural police holds *Conference Calls with Internet Service Providers* to exchange information about cybercrime trends and methods.

The NPA has set the month of April or May as the "public relations" month to promote information security policy to prevent cybercrime, and to raise the level of awareness for information security with the police, local government, schools and industries.

In **Korea**, pursuant to the *Act on Telecommunication Network Usage Facilitation and Information security* of 2002, audits are performed on information security management systems in telecommunications companies, and certificates are issued according to the result of the inspection, to improve the level of information security management. *Corporate Information Security Guidelines* have been published, a booklet which contains information on security solutions and successful adoption of services to help companies in putting in place an information security system. Korea has also designated a *Hacking and Virus Prevention Day* (the 15th day of each month) jointly with security companies, and organises a ceremony where participants can download vaccine programs for free. Pursuant to the *Act on Telecommunication Network Usage Facilitation and Information Security*, the Ministry of Information and Communication (MIC) has deployed 'Culture of Security Campaigns' to raise the security awareness level of Internet users. To foster a culture of security, it is carrying out events such as 'slogan and poster competitions' for elementary and junior high school students, and 'street campaigns for information security'. Furthermore, in order to promote information security in small and medium-sized enterprises, the MIC carries out on-site security check-ups and education for 1 000 participating companies, distributes information security practice instructions, and offers financing and tax relief for investments in security products and services.

In **Norway**, the *Norwegian Post and Telecommunication Authority* (NPT) arranges different forums/seminars, and sets up information portals. NPT also participates in *ad hoc* working groups.

The **Spanish** ASIMELEC[155] initiative has conducted a series of 21 road shows on security and trust in telecom networks all over Spain, supported through a government framework programme.[156]

Furthermore, the *Centro de Alerta Antivirus* has public and private collaborating partners, including 30 universities, 11 autonomous governments, and the Ministries of Foreign Affairs, Justice, Public Administration, Education, Culture and Sports. Additional investigation centres are co-ordinated by the CSIC (*Consejo Superior de Investigaciones Científicas*).[157] RED.es offers the "Secure Navigation" Web

154. The Japan Computer Emergency Response Team Coordination Center.

155. ASIMELEC is an industry association in Spain; cf. www.asimelec.es

156. Cf. www.setsi.min.es/progarte/arte.htm

157. This Alert Center has as an objective to become a platform for information exchange between users and experts in the security field, *e.g.* on computer viruses, and the documentation of their characteristics.

site[158] to increase trust in the Internet. This service is aimed at citizens, be they children, parents, or adults, for navigation of the Internet without concerns regarding unlawful or inadequate content. A new Web site specifically targeting children[159] provides links to a variety of educational leisure content, suitable for children between 6 and 12 years, to enable them to explore parts of the Internet under supervision of experts. This service also comprises means for Internet users to flag illegal content (in particular, child pornography).

In the **United Kingdom**, several government departments have outreach activities:

- The *Department of Trade and Industry* (DTI) promotes good information security management to all companies, but with a particular focus on smaller companies.[160] DTI also issues advice on authentication.[161] In addition, local business advice and support centres (the "*Business Links*") are the key vehicle for the delivery of a range of best practice messages.[162] DTI also raises awareness of the issues through surveys undertaken in partnership with the private sector.[163]
- The *Central Sponsor for Information Assurance* (CSIA) manages the co-ordination of outreach activities and leads on issues relating to home users and information to a general audience.[164] It also works closely with representative bodies of the UK local authorities.
- The *National Technical Authority for Information Assurance* (CESG) offers advice to government departments and the private sector information security supply industry, and a range of services including the management of the common criteria assessment process in the United Kingdom, the assessment of cryptography-based technologies and training and assessment of security service providers to the government.[165]
- The activities of the *National Infrastructure Security Co-ordination Centre* (NISCC[166]) include outreach to the management of the critical national infrastructure and to key players in those businesses and others who would benefit from information sharing activities. The WARP and ITsafe [cf. 2b) above] could also be considered as outreach.
- The National High Tech Crime Unit (NHTCU) undertakes a range of crime prevention activities aimed primarily at those users most at risk of online criminal activity.[167]

Outreach activities are also performed by other public bodies and the private sector (*e.g.* some ISP sites, the BBC, APACS[168] etc). A non-governmental organisations (NGO) survey of all collective private

158. http://navegacion-segura.red.es

159. http://chaval.red.es

160. Cf. www.dti.gov.uk/bestpractice/infosec

161. Cf. www.dti.gov.uk/industries/information_security

162. Cf. www.businesslink.gov.uk

163. Cf. www.dti.gov.uk/industries/information_security/downloads.html

164. Cf. www.cabinetoffice.gov.uk/csia

165. Cf. www.cesg.gov.uk

166. www.niscc.gov.uk

167. Cf. www.nhtcu.org/nqcontent.cfm?a_id=12307&tt=nhtcu

168. APACS, the UK payments association, is a trade association for institutions delivering payments services to end customers. Cf. www.apacs.org.uk

sector initiatives has been published.[169] The government regularly works in partnership with NGOs to reach specific audiences. Typical current projects are the collaboration between DTI and the Institute of Directors to produce an infosec publication and the joint work of the Confederation of British Industry (CBI), Ernst & Young, and the DTI to produce a manual for CBI members.

A public relations campaign (operating under the working title of "Project Endurance") is planned to be launched in autumn 2005 to make home users aware of the risks of cyberspace and the actions they can take.[170]

From the **United States**, several initiatives for government outreach across sectors were reported:

- The NCS's outreach to the private sector through public-private partnerships includes the NCC Telecom ISAC, NSTAC, and the NSIE. These partnerships provide forums for two-way information sharing between industry and government, as well as amongst members of industry.
- The IP's Infrastructure Co-ordination Division (ICD) and National Communications System (NCS) division facilitates NCSD's outreach to specific critical infrastructure and key resource sectors.
- The NCSD's outreach to the private sector through public-private partnerships includes the National Cyber Security Partnership (NCSP), and the National Cyber Security Alliance (NCSA).[171]
- NIST participates with the US Small Business Administration, the US Federal Bureau of Investigation (FBI), InfraGard (an FBI program), the US Chamber of Commerce, and the National Cyber Security Alliance in an outreach effort to small and medium-sized businesses. This outreach project focuses on raising awareness and knowledge of information security issues within these businesses, and providing them with practical, cost-effective tools and techniques for improving their information security efforts.
- The Department of Justice is a frequent speaker on computer and network security issues and cybercrime enforcement at industry events. In addition, the Department has worked with various industry partners to establish protocols for reporting cybercrime and working with law enforcement during criminal investigations. Additional information on the Department's cybercrime activities can be found at the CCIPS' Web site, www.cybercrime.gov.
- Since August 2002, the FTC has been conducting a multi-faceted education campaign to increase public awareness of the importance of good information security practices. The target audience for this campaign includes consumers, children, and businesses. To reach as many people as possible, the FTC participates in numerous partnerships and works with representatives from a variety of consumer groups, trade associations, non-profit organisations, corporations, and government agencies.[172]

169. Cf. www.intellectuk.org/groups/saint/Review_Information_Assurance.pdf

170. This project is the most significant public-private partnership in this area. Aside from key Government Departments and the NHTCU, a wide range of private sector interests are contributing money and other resources to this project. Contributors include Microsoft, e-Bay, Dell, MessageLabs, Lloyds TSB, HSBC and Secure Trading.

171. Additional detail on NCSD participation in and co-operation with the NCSP and NCSA is provided in response to question 8a below.

172. More information on this education campaign is provided in the response to question 3 below.

f) Outreach to state and local government

The **Australian** *High Tech Crime Centre's* (*AHTCC*) training initiatives, designed to improve the knowledge and capacity of Australian Police to investigate instances of high-tech crime, have been extended to some Commonwealth regulatory agencies. Furthermore, state and local governments are represented on the *Trusted Information Sharing Network* (TISN) peak body and attend meetings of critical infrastructure sector groups.

In **Austria**, a committee (the "Länderarbeitsgruppe") has been established for co-ordination between the federal states and with the ICT-Board, which meets on a regular basis. In the ICT-Board several policies, specifications, decisions have been agreed. Through the close co-operation with the federal states, there is also significant outreach to local governments, cities and municipalities. For example, the Internet-Policy and the E-Mail-Policy, and specifications mentioned above are also applied by those parties.[173]

In **Canada**, the Public Sector Chief Information Officer (CIO) Council has had a National Sub-Committee on Information Protection (NCSIP) in place for at least five years. This group, comprised of representatives from the federal government, provincial CIO offices and municipalities, is a forum for exchanging information and sharing best practices. Industry Canada works with this group to obtain views and input to its policy work in the area of security.[174]

In **Denmark** all public institutions are obliged to offer confidential communication using digital signatures since 1 February 2005.

In **Finland**, the information security instructions of the Government Information Security Management Board (VAHTI) are increasingly used also by local government. These instructions, besides being publicly available on the Internet, are posted to all municipalities, and are also used in local authorities' seminars.

In **France**, no action has at this stage been taken with regard to sub-national government. Nevertheless, local entities of the public administration do have access to all of the methodological tools that the DCSSI has made available on its Internet site.

In **Germany,** the *German Administration Network* (DVN) serves as the communication network for federal and federal-state (*Länder*) administrations. It defines rules and standards for availability and confidentiality of communications between administrations in Germany in a joint network. Furthermore the federal government advocates an integrated e-government landscape in Germany and calls for intensive co-operation between the federal government, federal-state governments and municipalities. The "virtual post office" (VPS) was developed within the framework of the BundOnline 2005 initiative in order to enable secure electronic communications. Since 2004, the virtual post office has been available to all the federal authorities as well as federal-state governments and municipal administrations.

---

173. The municipality of Vienna and the state of Styria are both participating actively in the efforts for standardisation of ICT technology of the Federal Government of Austria, represented by the Chief Information Office, in particular in the process of standards for a secure ICT environment for A2A, A2B and A2C applications. The main focus is on *i*) Establishment of electronic and advanced electronic signatures for citizens, administrations and business (www.buergerkarte.at, www.signatur.rtr.at/); *ii*) Secure and reliable transportation of information; and *iii*) Methods to standardise the transaction between the partners of all levels in a secure and legal way (http://reference.e-government.gv.at/).

174. The NCSIP meets three times a year and holds monthly teleconferences. In addition, federal, provincial, municipal weekly conference calls are held to discuss emerging threats, vulnerabilities and incidents. These calls are co-ordinated by the Federal Department of Public Safety and Emergency Preparedness (PSEPC).

In **Japan**, *guidelines which prescribe basic concepts, implementations, operations and review procedures* have been developed in 2001 for local governments to assist them in taking information security measures. Local governments are obliged to take into account information security in their operations. In addition, *fiscal measures* are being implemented for local governments, to enable them to buy the equipment required to enhance network security.

In order to streamline the administration, the **Korean** Government has established the *Act on Electronic Government*. In 2003, the Korean Government improved the relevant law system to re-enforce the security of IT systems operated by government agencies under the 'Information Security System Construction Plan' within the "e-Government Roadmap", and has been offering financial and technical support to local governments to achieve this goal.

In **Spain**, the ASIMELEC[175] initiative has received support under a government framework programme (www.setsi.min.es/progarte/arte.htm), to realise a series of 21 road shows on security and trust in telecom networks all over Spain. The *Centro de Alerta Antivirus* has public and private collaborating agents, including 30 universities, 11 autonomy governments, and the Ministries of Foreign Affairs, Justice, Public Administration, Education, Culture and Sports. Other investigation centres are co-ordinated by the CSIC (*Consejo Superior de Investigaciones Científicas*).

In **Sweden**, the IT Incident Centre has been established with the following intended constituency: government authorities, regional authorities, municipalities and companies.

In the **United Kingdom**, the Central Sponsor for Information Assurance (CSIA[176]) works closely with representative bodies of the UK local authorities.

In the **United States**, the NCS's outreach to state and local government primarily focuses on educating them about priority service programs that provide emergency service users with priority access to wireline (Government Emergency Telecommunications Service), wireless (Wireless Priority Service) telecommunications services during crisis, as well as priority restoration and provisioning of services (Telecommunications Service Priority). In addition, the NCSD has established a relationship with the *Multi-State Information Sharing and Analysis Center* (MS-ISAC) for information sharing and outreach to state and local governments regarding cyber security issues.[177] The Department of Justice provides education and training to all federal law enforcement agencies, as well as to state and local law enforcement. Training includes prosecutorial and investigator training for cybercrime, *e.g.* on investigative techniques, computer forensics and other issues in electronic evidence. Further investigative training is offered by the FBI, and also by other federal agencies that maintain computer forensic and electronic evidence-handling capability.

g) Education and training

The **Australian** High Tech Crime Centre (AHTCC) has conducted a range of training initiatives designed to improve the knowledge and capacity of Australian Police to investigate instances of high tech crime. This training has also been extended to some Commonwealth regulatory agencies (see www.ahtcc.gov.au).

175. ASIMELEC is an industry association; cf. www.asimelec.es

176. Cf. www.cabinetoffice.gov.uk/csia

177. One specific joint NCSD and MS-ISAC initiative is a series of national Web casts that examine critical and timely cyber security issues. Additional information on NCSD participation in and co-operation with the MS-ISAC is available in the response to question 8a.

The **Austrian** University of Technology in Graz (for Applied Information Processing and Communications – IAIK[178]) offers a special course package "Security in Information Technology" for graduate students. The University of Klagenfurt also provides teaching with a specialisation in IT-security.[179] Other universities (Vienna, Linz, etc.) also offer classes for students in the field of security. Furthermore, there are also institutions from the private sector (*e.g.* www.wifiwien.at) which offer classes within the field of IT-security as well.

In **Canada**, education and awareness activities are underway within the private sector and the various levels of government. While there is no single entity co-ordinating these initiatives, there are complementarities among them, with each sector focussing on their particular areas of interest. For example, governments have introduced numerous initiatives aimed at ensuring the level of security in their networks is appropriate and at ensuring that employees are aware of the need for good security practices in the work environment. In addition, those departments that have consumer protection mandates have embarked on various campaigns to provide consumer education relative to reducing identity theft online, the need to keep passwords/PINs confidential, the threats posed by phishing, and spyware etc. These public sector initiatives are complemented by various others within the private sector. Various organisations with an interest in security are convening conferences and discussion fora to discuss security issues and explore solutions to them. At these conferences, the vendors are making white papers and information about the latest in security products and services available to all attendees and delegates. The financial services sector has been particularly active in this regard.

Finland foresees training activities for employees in the public sector as part of the yearly planning. These measures are supported by electronic publications prepared by the *Government Information Security Management Board* (VAHTI), which has published *guidelines* on the issues, and conducts an ongoing education programme on how to promote information security awareness In particular, the Finnish government has published detailed guidance on information security for employees in the public sector in the "User's Information Security Instruction" prepared by VAHTI in 2003. This instruction is used widely in all sectors in Finland.[180]

To help prepare for the National Information Security Day, a Web service designed to support information security teaching in comprehensive schools was launched on 15 November 2004, and was widely publicised among teachers.[181] Various teaching, ICT, information security, law and child welfare professionals were involved in setting up the Web service. It contains separate sections for teachers, younger and older children, and parents. The teachers' section includes readily comprehensible teaching material on information security. The material is presented in an illustrated and convenient form and it can also be printed out if necessary. Links allowing teachers to find more details on information security technologies are available.[182] The service also includes an option ('Kummipankki') for requesting an information security expert to come and talk to teachers and parents free of charge about the basics of secure Internet use, for instance at teachers' meetings, parents' evenings and meetings of parents associations. These information security experts are representatives of the various participants in the project. The sections of the Web service designed for comprehensive school students make good use of the

178. www.iaik.tu-graz.ac.at

179. Cf. www.ifi.uni-klu.ac.at/IWAS/PH/

180. This instruction can be found on the Web at the pages of the Ministry of Finance (in Finnish language at www.vm.fi/vahti; in English at www.financeministry.fi/security; and in Swedish at www.finansministeriet.fi/datasakerhet), and on the OECD "Culture of Security" Web site (www.oecd.org/sti/cultureofsecurity/).

181. Available in both Finnish and Swedish; cf. www.tietoturvakoulu.fi

182. For example see www.tietoturvaopas.fi (Finnish and Swedish).

diversity of the Internet. Stories targeted at different age groups have been designed as cartoon-like animations and incorporate information security advice, points to mull over, and lots of different tasks. On the National Information Security Day (8 February 2005), an information security competition will be launched, open to all comprehensive school pupils in Finland (*i.e.* up to the ninth grade). The winners will be announced at the end of the school year.

France organises training sessions for government employees on security of networks and information systems under the responsibility of the *Information Systems Security Training Centre* (CFSSI), a unit of the Central Directorate for Information Systems Security (DCSSI). This activity builds IT security competencies in the public sector and contributes directly to the development of a "culture of security", and aims to:

- Provide customised IT security training for different types of public sector players (managers, designers and end-users).

- Create a network of interchange and mutual enrichment in the realm of information system security training with universities and specialised institutions of higher education.

The activity is carried out by a small (3-person) team that organises training sessions, which may be:

- Short day-long courses (lasting one-to-three days): building awareness of IT security, the EBIOS method of risk assessment, security and the Internet, and PKI.

- Practical training in IT security: two days for end-users; five days for administrators.

- Short-term courses in three different subjects (lasting between two and six weeks): cryptography, IT security, compromising signals.

- A certified advanced study in information systems security (BESSI – two years, including one year spent on a scientific project).

The teaching staff is composed of university professors; instructors, engineers and officials from the DCSSI; as well as teaching assistants and lecturers from various Ministries and businesses. The groups targeted are civil servants so as to build awareness and develop IT security competencies in the public sector.[183]

The Federal Government in **Germany** considers training to be a key issue for protection against risks. As a result of a nation-wide project group, further training programmes in the area of prosecution of information and communication technology crime will be standardised. Training of multipliers is foreseen as a first step, followed by specialist courses (for example, co-operation with the US-based "International Association of Computer Investigative Specialists" – IACIS).

In **Japan**, the Ministry of Internal Affairs and Communications (MIC) supports education and training measures, carried out by a private organisation to foster the education of specialists for information security management.

Korea reported an *international incident response co-ordination drill* with the participation of China, Japan and Korea in the second half of 2004, organised in the framework of the first 'China-Japan-Korea

183. In 2003, some 1 200 hours of instruction in IT security were held, with overall 900 participants. For further information, cf. www.formation.ssi.gouv.fr.

Working-level Meeting on Telecom Network Security and Information Security'. Since 2001, the Ministry of Information and Communication (MIC) has been operating the 'Online Information Security Training Lab', where information security managers are offered various technology training programs to enhance their abilities to prevent and respond to security incidents. MIC has also been holding an annual academic conference entitled 'Symposium on Information Security' since 1996. Furthermore, Korea has been operating a qualifying examination scheme for nationally certified 'Specialist for Information Security (SIS),' to solidify the base for certifying and training information security experts. Korea also supports training measures for officials in charge of informatisation in developing countries of the Asia Pacific region.

In the **Netherlands**, some of the most relevant programmes include those of the Government Education Institute (*Rijksopleidingsinstituut*, ROI), which provides education and training programmes for employees in the public sector. One of its programmes, named "Innovative Government" (*Innovatieve Overheid*), contains two (of eight) sub-programmes dedicated to e-security issues. Another sub-programme on "Reliable Communication and Information provisioning" (*Betrouwbare Communicatie en Informatievoorziening*) is based on the Public Key Infrastructure (PKI) programme for the government. During the course, the objectives and added-value of PKI, as well as the implications of PKI for the organisation in question are being explained. Furthermore, another subprogram titled "Hands on Working with the Internet" includes an implicit link to e-security.

In addition, several (technical) universities and academies offer education programmes in the domain of e-security: The Technical University Eindhoven offers a Master's programme on Information and Security Technology, providing essential tools for secure communication and data protection. The technical University Delft provides a programme on encryption, and the Academy The Hague (*Hogeschool Den Haag*) offers a Master of Business Administration in Security Management.

Some IT-sector organisations and commercial firms (*e.g.* KPMG, Getronics) provide training, courses and workshops regarding IT and e-security as well. The *Netherlands Society Information Security* (*Nederlands Genootschap voor Informatiebeveiliging*, NGI) is an active branch organisation providing workshops and meetings with regard to topical security incidents like phishing and hacking. The target groups are IT managers of which the majority is working in the public sector. The NGI is working close together with ECP.nl, the Platform for Information security (*Platform voor Informatiebeveiliging*) and with academies. A large e-security fair will be organised in May 2005 (www.ib-markt.nl) with briefings, workshops and a marketplace. Another example is "Security Plaza", a part of "Media Plaza", which is a demonstration centre for multimedia offering one day courses about application security aimed at employees working both in the public and private sector, and carrying responsibility for e-security issues in their organisation.

In **Spain**, the initiative by ASIMELEC (an industry association; cf. www.asimelec.es), has received support in a government framework programme[184] in order to realise a cycle of 21 roadshows on security and trust in telecoms networks all over Spain. Furthermore, the *Centro de Alerta Antivirus* has public and private collaborating agents, including 30 universities, 11 autonomy governments, the Foreign Affairs Ministry, the Justice administration, other bodies of the public administration, and other investigation centres co-ordinated by the CSIC (*Consejo Superior de Investigaciones Científicas*). This Alert Center was founded with the objective to become a platform for exchange of information between users and experts on security issues, *e.g.* on the different viruses on the Internet, and document their characteristics. In addition, the Web site of RED.es, named *Secure Navigation* (http://navegacion-segura.red.es) is aimed at increasing confidence in the Internet with the population at large, including children, parents, adults, etc., to allow them to navigate the network without fear to find unlawful, or inadequate content. Moreover, a new Web

184. Cf. www.setsi.min.es/progarte/arte.htm

site *chaval.es* (http://chaval.red.es), specifically for children, contains links to a variety of educational and leisure content, targeting children 6 to 12 years old, and enabling them to explore parts of the Internet, under expert supervision. This site also includes means for Internet users to flag unlawful content (in particular, child pornography).

In the **United Kingdom**, the *Central Sponsor for Information Assurance (CSIA)*, the lead body for the United Kingdom in the area of education and training in the area of information security, is working with Becta (British Educational Communications and Technology Agency) on education and training issues and initiatives .[185] At institutions of higher education, there are an increasing number of specialised information security courses available, as well as security modules in a range of business and IT courses.[186] Training is dispersed by a vast array of training providers, and some courses are accredited by providers of qualifications – *e.g.* the Information Systems Audit and Control Association (ISACA).[187] Training for government information security staff is available through the Infosec Training Paths and Competencies Scheme.[188] Additionally, it is being discussed how to increase the professionalism and professional standing of experts in information security, including the possibility of creating a new professional body to achieve these goals.

In the **United States**, the two key documents produced by NIST to support training and education are:

- Special Publication (SP) 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model.

- SP 800-50, Building an Information Technology Security Awareness and Training Program.

NIST hosts the Federal Information Systems Security Educators' Association (FISSEA), an organisation run by and for Federal information systems security professionals. FISSEA assists Federal Agencies in meeting their computer security training responsibilities, and strives to elevate the general level of information systems security knowledge for the Federal Government, and the federally related workforce. It serves as a professional forum for the exchange of information and improvement of information systems security awareness, training, and education programmes. It also seeks to provide for the professional development of its members.

h) Science and technology (S&T) and research and development (R&D)

Austria has at present no co-ordinated government initiative, while supporting a variety of S&T and R&D projects in the country. Security is an important focus for several research institutions in Austria, usually more focused on basic research, while co-operating with industry and government, *e.g.* in the area of digital signatures, where the technical competence for verifying the security of soft- and hardware solutions for public approval comes directly from universities (IAIK and A-SIT). Others are involved in

185. The following CSIA publications include details of related education and training issues and initiatives: "Protecting our information systems" (www.cabinetoffice.gov.uk/csia/documents/pdf/CSIA_booklet.pdf) and "Information Assurance: a review of UK Government and industry Initiatives" (www.cabinetoffice.gov.uk/csia/documents/pdf/Review_of_Information_Assurance_v3_11_04.pdf).

186. For example, at the Royal Holloway University of London (www.isg.rhul.ac.uk), the London School of Economics (www.isig.lse.ac.uk), Cambridge University (www.cam.ac.uk), Northumbria University (www.northumbria.ac.uk), Glamorgan University (www.glam.ac.uk) and Leeds University (www.leeds.ac.uk).

187. www.isaca.org

188. Cf. www.cmps.gov.uk/courses/course.asp?id=15282

integrating cryptography into general tools[189] to facilitate widespread use and increased awareness of security. The Austrian computer society (OCG) organises research and the transfer of results to businesses.[190]

The Institute for Applied Information Processing and Communications (IAIK; www.iaik.tu-graz.ac.at) at the University of Technology in Graz (www.tugraz.at) works in three main areas: Applied research in *e.g.* computer networking, embedded systems, system-on-chip design, computer security, and information security. IAIK emphasises an integrated view between these areas.

At the University of Klagenfurt, the research group "Systems Security" (syssec; www.ifi.uni-klu.ac.at/IWAS/PH/) focuses on the security of complex IT-systems. Founded in 1997, its research areas include applied cryptology, security infrastructures, key management, multi-party computation, and security tokens. In particular, research is conducted on the following topics:

- Security concepts and their basics.
- Mathematical fundamentals of cryptology.
- Design and analysis of cryptographic mechanisms.
- Key-management and authentication.
- Applied cryptology.
- Security in distributed systems and networks.
- Technical data protection and information security.
- Security tokens (especially Smartcards).
- Secure applications for Personal Digital Assistants (PDAs) and smartcards.
- Trust-Centers and security infrastructures.
- Digital signatures, liability, and non-repudiation.
- Tele-co-operation and eCommerce.
- Security in multimedia systems.
- Multi-Party computation.
- Security concepts in document management.
- Implementation of prototypes of developed or studied mechanisms.

In **Canada**, the Computer Science faculties of various universities are examining issues associated with security and privacy in information networks. A number of these universities have launched collaborative initiatives with the private sector to identify research needs and together they are defining a research agenda for Canada in this area. Most recently, Dalhousie University (Province of Nova Scotia) has announced that it will be establishing a centre for privacy and security. The University is partnering with the private sector in this initiative (*e.g.* Symantec) as well as the various levels of government. To complement the centre's various education initiatives, a research lab will be established. The University of New Brunswick has been working on a similar initiative.

The **French** Directorate-General for Enterprises in the Ministry of Economics, Finance and Industry, launched calls for projects in connection with a programme to finance information systems security R&D in 2001, 2003 and 2004. The purpose of the programme ("Oppidum"[191]) is twofold: *i*) to promote innovation in the sector; and *ii*) to foster trust in tools for the development of the information society.

189. *e.g.* at the University of Linz in the "CodedDrag" project, cf. www.fim.uni-linz.ac.at/research/CodedDrag/

190. www.ocg.at/ueber-uns/arbeitskreise/it-sicherheit/akit.html

191. www.telecom.gouv.fr/oppidum/

Successive calls for projects have put an emphasis on the following three major aspects of information systems security:

- Digital identity.
- Systems of electronic transactions.
- Security tools for networks and terminal equipment.

In the 2004 call for projects, 18 were selected from 45 submitted. They cover the following areas:

- Parental control filters.
- Techniques for securing terminals.
- LAN security tools.
- Smart cards.
- Electronic signature and archiving tools.

Industrial and technological research networks are also supported in a number of projects relating to security systems, software and components.[192]

The **German** Federal Ministry of Education and Research (BMBF) sponsors several IT-research and development projects. One is the "MIND" project for the development of new methods for detecting and preventing intrusion into computer systems via the Internet. Other partners in the project are the Fraunhofer Gesellschaft (FhG FIRST) as the leading partner, Siemens, IT Service Omnikron and the St. Petersburg-based "Institute for Information and Automation".

Japan reports comprehensive R&D to ensure the network security and reliability, in particular on the following topics:

- Implementations of technologies for prevention and detection of cyber terrorism.
- Implementations of technologies for analysis of unknown cyber attack in real time.
- Advanced network authentication infrastructure technology for secure and safe provision and use of services.
- Cryptographic technology.
- Time stamp and platform technology.

The **Korean** Government is carrying out information security-related R&D activities and standardisation in accordance with the *Framework Act on Informatisation Promotion*. The Korea Information Security Agency (KISA), the National Security Research Institute (NSRI), and the Electronics and Telecommunication Research Institute (ETRI) are the main actors in developing information security-related technologies such as cryptography, biometrics, wired/wireless network security management, RFID, high-tech infrastructure security, and computer security incident prevention.

In **Norway**, the Gjøvik University College offers a master's degree in information security. The *Norwegian Post and Telecommunication Authority* (NPT) participates in the EU Framework Programme 6 project OBAN (Open Broadband Access Network). One of NPTs goals is to look into the security issues of new mobile services.

192. Cf. www.telecom.gouv.fr/reseaux/index.htm

In **Spain**, the PROFIT programme[193] is a special tool for the government to offer a variety of public aid, to stimulate the business sector to perform research and development activities, in accordance with the Spanish National Scientific Investigation Plan for Research and Development (I+D+I) 2004-2007. Under this program, the Industry, Tourism and Commerce Ministry has created an action line named "Strategic horizontal Action for security and confidence in Information and Communications Systems and Information Society services", which has as an objective to promote technical investigation focused on security enhancing information and communications systems.

In the **United Kingdom**, research and development is funded through several sources depending on the nature of the research being undertaken. The *Engineering and Physical Sciences Research Council*[194] is part of the top level research funding bodies in the United Kingdom and makes funding available for network and information security issues. It is funded by the Department of Trade and Industry (DTI) as part of its overall research and technology activity. The DTI also undertakes "Foresight" work which attempts to give direction to research work by reaching a consensus view on the societal issues to be addressed, including a recent project on Cybercrime and Cybertrust.[195]

In addition, DTI also works in the sphere of innovation to disseminate ideas emerging from the science base.[196] DTI also does research on information security breaches and the response by UK companies in terms of technology and process. This "Information Security Breaches Survey" was last published in 2004 and forms a key part of DTI's promotion of information security as a business enabler and a business issue.[197]

The *Central Sponsor for Information Assurance* in the Cabinet Office (CSIA) oversees a research and development budget called "common good" funding which is designed to develop security solutions of broad applicability within central government and the wider public sector. The *National Infrastructure Security Co-ordination Centre* (NISSC) has a research budget to help it address issues relevant to its mission to protect the critical national infrastructure from electronic attack. The *National High Tech Crime Unit* (NHTCU) and the Home Office undertake research into incidents of cybercrime.

In the **United States**, the NCSD co-ordinates with DHS's Science and Technology Directorate (S&T), which is responsible for prioritising and implementing the Department's research and development programmes. The White House Office of Science and Technology Policy (OSTP) established a Critical Information Infrastructure Protection Interagency Working Group (CIIP IWG) under the National Science and Technology Council currently engaged in developing R&D plans in response to the US National Cyber Security Strategy and the Presidential Directive HSPD-7. Furthermore, NIST is actively engaged in information security research and development. Some topics of research include:

- Smart card technologies.
- Biometrics.
- Automated security testing.
- Quantum cryptography.

193. www.min.es/profit

194. www.epsrc.ac.uk

195. Cf. www.foresight.gov.uk

196. In the past, there have been programmes such as the Management of Information programme which had a strong information security component. The DTI is now developing a technology strategy to focus its efforts in innovation and it is expected that the strategy will include a cross-cutting theme on security.

197. www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf

- Security of voice-over-IP systems.
- Digital forensics.

NIST has also developed tests for cryptographic modules and algorithms and authorisation management and access controls.

i) International outreach and co-operation

Australia has mutual assistance agreements with a number of countries. The Australian Federal Police has an international liaison network for dealing with international crime. The Australian High Tech Crime Centre (AHTCC) acts as a hub to assist this co-operation and links state law enforcement agencies, other Australian Government agencies and overseas agencies such as the Interpol, the US Federal Bureau of Intelligence and the UK's High Tech Crime Unit. Australia has also established relations with regional neighbours to protect its information infrastructure.[198] In addition, the Australian Government is leading efforts to enhance e-security within the Asia-Pacific region. In APEC, Australia is leading initiatives to build CERT capacity and raise awareness of the value of CERTs in developing economies through APEC's Telecommunications and Information Working Group – APEC TEL.[199] The eSecurity Task Group (eSTG), part of APEC TEL and currently chaired by Australia, is fostering regional co-operation on e-security issues of common interest, such as PKI, authentication, security of systems and networks, assisting small business and home users with their security needs, strategies for fighting cybercrime, and the development of CERT capability in the region. With co-funding from the Australian Aid Agency, AusAID, the Attorney-General's Department has co-ordinated a CERT Capacity Building Project (CERT Project) taking 'in-country' CERT capacity building training to Papua New Guinea, the Philippines, Thailand, Vietnam and Indonesia.[200] As regards international standards, Australia has been working with bodies such as the International Telecommunication Union to ensure that security is 'built in' to software and hardware, rather than being 'bolted on' as an afterthought.

Austria mentions international co-operation initiatives foreseen under European law, in particular in a number of EU directives which address IT security, or have impacted national transformations in Austria with IT-security relevance, in the areas of protection of personal data, digital signatures, and electronic

198. The AHTCC works closely with like-minded international high tech crime law enforcement agencies in relation to investigations, intelligence development and capability building, and has commenced a project of law enforcement high tech crime capacity building within the Asia Pacific region.

199. Cf. www.apectelwg.org/

200. The CERT project also funds the development of guidelines for establishing CERTs and provides funding for a CERT communications network to allow regional CERTs to exchange alerts and advisories. In addition, Australia is overseeing an APEC and USA funded project to allow in-country CERT training to be provided to Chile, Peru, Mexico and the Russian Federation. The objective of these closely linked projects will be the creation of a network of CERTs throughout the Asia-Pacific region which will be able to exchange information on IT security issues quickly and securely. This network will then be able to exchange information with similar groups being created successively in other regions.

commerce.[201] As an example, EU supervisory authorities for electronic signatures co-operate in the Forum of European Supervisory Authorities for Electronic Signatures.[202] Furthermore,

- The "Secure Information Technology Center" (A-SIT)[203] interacts with other corresponding institutions at the international level, as laid down in the statutes of the association ("appropriate international co-operation").
- The "National Computer Crime Unit – Austria", part of the *Bundeskriminalamt* (Criminal Intelligence Service Austria) works closely together with Interpol.
- The "Computer Incident Co-ordination Austria" (CIRCA) has international outreach activities through the "Internet Service Providers Austria" association (ISPA),[204] and through A-SIT.
- The Federal Chancellery of Austria will establish the BCS (Business Continuity System) for the EU "New, Second Generation Schengen Information System" (SIS II), and for the EU Visa Information System (VIS).[205]
- Austria participates in the EU "Information Society Working Group" of the European Union, which also addresses IT security as part of its work.[206]

Canada participates in the *Group of Eight (G8) 24/7 network* and provides a point of contact in the Royal Canadian Mounted Police (RCMP) to assist other countries in the investigation of computer crime. Canada also works with other countries through mutual legal assistance efforts, to co-ordinate the investigation of activities linked to information technologies. Canada is also active in international law enforcement activity such as the *G8 High Tech Crime Group* (the Lyon Group), and it has chaired meetings and hosted activities. It is also a signatory to the *Council of Europe Convention on Cybercrime* (and was active in its drafting). Canada has also provided significant leadership in developing a National Computer Security Incident Response Team *(CSIRT) Watch and Warning Network in the Americas* though efforts in the Organisation of American States (OAS).

The **Czech Republic** participates in the OECD Working Party on Information Security and Privacy, the OECD Spam Task Force, the Forum of European Supervisory Authorities for Electronic Signatures (FESA), the European Network and Information Security Agency (ENISA), NATO, and in different

201. Austria specifically referenced *i*) Directive1995/46/EC of the European Parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; *ii*) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 — on a Community framework for electronic signatures; and *iii*) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 — on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

202. FESA, cf. www.fesa.rtr.at. The mission of FESA is co-operation in cross-border cases and to provide for a harmonised interpretation of national laws on electronic signatures in EU member countries. FESA members meet three times a year, discuss current issues, and develop common views. FESA currently consists of 21 bodies from countries which have to transpose Directive 1999/93/EC (*i.e.* EU and EEA member countries, and EU candidate countries).

203. Cf. www.a-sit.at

204. Cf. www.ispa.at/

205. At the EU Council of Justice and Home Affairs meeting in June 2003, the Council decided that the SIS II and VIS systems should not be based only on one central data base system at one location. The Federal Chancellery of Austria offered the location of the ZAS as a business continuity system for SIS II and VIS.

206. Cf. http://europa.eu.int/information_society/index_en.htm

programmes of the European Union [IDA (IDABC) – Interoperability framework, TESTA, Security, e-Link, and in the "Safer Internet Action Plan Plus".

Denmark participates in an EU informal working group on Spam related issues, in the OECD working group and task force on spam, and in the NATO CCPC (Civil Communication Planning Committee).

In **Finland**, active participation in international information security co-operation is ranked as a top priority in the Government Information Security Development Program and in the National Information Security strategy, which both contain specific projects to develop Finnish participation.

In **France**, the DCSSI is an active participant in international working groups in the field of information systems security within a variety of international bodies (European Union, G8, OECD, UN). In addition, the DCSSI is taking part in the start-up of the European Network and Information Security Agency (ENISA), which was established in March 2004. France is also one of the first countries to have joined the 24/7 network initially instituted by the G8, which today links 35 countries.[207] France has signed the Convention on Cybercrime of the Council of Europe,[208] participates in international co-operation amongst CERTS through EGC, TF-CSIRT and FIRST, and is a signatory to two agreements concerning recognition of security certificates for IT products and systems.

In **Germany**, to enable cross-border prosecution of criminal offences in data networks, offences of an international nature are reported by the specialist units in the Federal Criminal Police Office via Interpol to the countries concerned, so that separate investigations can be launched. Within the framework of international efforts to combat Internet crime, the Federal Criminal Police Office is also represented in the "Interpol European Working Party on Information Technology Crime",[209] the "Europol Cybercrime Expert Meeting",[210] and the "G8 High Tech Crime Subgroup".[211]

Japan reported initiatives in the framework of multilateral meetings such as APT[212] and APEC, as well as on a bilateral basis, *e.g.* with the United States, China, and Korea. More specifically:

- "Telecom-ISAC Japan", established by Japanese ISP and vendors as a private organisation that collects, analyses and shares security information among members, co-operates with other corresponding organisations in other countries.

207. This cross-border network, which the member countries can activate at any time, should facilitate contacts in the event of an emergency. Moreover, the underlying idea of the network was incorporated into the Convention on Cybercrime of the Council of Europe.

208. A ratification bill is being examined in the French National Assembly.

209. Key areas of work are: exchange of experience, phenomenology, and project group work. The Federal Criminal Police Office in this context also serves as the National Central Reference Point on Information Technology Crime.

210. Key areas of work: exchange of experience and phenomenology.

211. Key areas of work: projects and exchange of experience. German agencies represented include the Federal Ministry of Justice (BMJ), the Federal Ministry of the Interior, the Federal Ministry of Economics and Labour (BMWA), the Federal Office for Information Security and the Federal Criminal Police Office. The Federal Criminal Police Office serves as Germanys´ High Tech Crime Point of Contact of the 24/7 network.

212. The Asia Pacific Telecommunity; www.aptsec.org

- JPCERT/CC, established in 1996 as a Computer Incident Response Team, supported the establishment of APCERT (Asian information security organisation) and co-operation among CERTs in the Asian region. In addition, JPCERT/CC is affiliated with FIRST which was established for the purpose of co-operation and information sharing between CSIRTs at the international level. In addition, IPA also co-operates with corresponding organisations in other countries.

- The National Incident Response Team (NIRT), established in the IT Security Office of the Cabinet Secretariat in April 2002, co-operates with foreign CSIRTs.

- The National Police Agency (NPA) holds "Seminars on Police Info-Communications" and invites police info-communication officials from developing countries to provide information and know-how with regard to police info-communications, including countermeasures against cybercrime. The NPA also holds conferences on technological aspects of the investigation of cybercrime in the Asian region.[213] Furthermore, since March 2001, the NPA has been operating a computer network (the "Cybercrime Technology Information Network System" - CTINS) to share and exchange technological and other information on the investigation of cybercrime among Asian countries (including nine countries and one region). Other co-operative efforts of the NPA with respect to cybercrime include the "G8 High-Tech Crime Subgroup", and Interpol.

The **Korean** Ministry of Information and Communication (MIC) consistently attends APEC and other cybercrime conferences to join the international efforts against cybercrime. In addition, Korea organised the first 'China-Japan-Korea Working-level Meeting on Telecom Network Security and Information Security'' in March 2004.[214] The Korean Information Security Agency (KISA) established a number of co-operative bilateral "information security agreements" with entities in the public and the private sectors in Australia; China; Germany; Hong Kong, China; Japan; and the United States.[215] Korea is participating in information security-related meetings at various international organisations such as APEC and the OECD. Korea has proposed a 'Strategy for Ensuring a trusted, secure and sustainable online environment' at the 31st APEC-Tel ESTG meeting, which has drawn support from the majority of the APEC member economies. Korea has also proposed to strengthen Cyber Security within the ASEM Region at the 5th ASEM summit, and held an ASEM Cyber Security Workshop in June 2005 in Seoul, which provided an opportunity to strengthen the co-operation between Asia and Europe. Korea has been stressing the roles and responsibilities of Government, enterprises, and the private sector regarding information security, and

213. The aim is to enhance international co-operation such as an efficient exchange of technical information on cybercrime among Asian countries.

214. This initiative *i.a.* operates a mailing list to exchange knowledge on information security (including cases of security violation), on traffic information, and on trends in Internet security among the three countries. Korea has also established TFT for 'China-Japan-Korea Network Monitoring Project' to share statistical information on network traffic among three countries. Furthermore, statistical information on network traffic is shared in the 'China-Japan-Korea Network Monitoring Project' and an international incident response co-ordination drill was conducted with the participation of the three countries in the second half of 2004. In addition, a task force on information security training and security violation response has been established, as well as training measures for officials in charge of informatisation in developing countries of the Asia-Pacific region.

215. Co-operating bodies under such agreements include the Australian Communications Authority (www.aca.gov.au), the CNCERT/CC of China (www.cert.org.cn), the Office of the Privacy and Freedom of Information Commissioner of the State of Berlin, Germany (www.datenschutz-berlin.de), the Hong Kong, China, Privacy Commissioner's Office (www.pco.org.cn); in Japan ECSEC (www.ecsec.org), IPA (www.ipa.go.jp), and JPCERT/CC (www.jpcert.or.jp); and in the United States Cisco Systems (www.cisco.com) and Microsoft (www.microsoft.com), as well as SEI and CMU (www.cmu.edu).

has been making efforts in establishing the co-operation system among CERTs around the world to enter into international agreements on cybercrimes and to cope jointly with Internet security incidents. Finally, Korea plans to carry out educational programmes to teach how to analyse and respond to security incidents, targeting private and public CERTs in the developing countries in the Asia-Pacific region.

Norway participates in information security initiatives within the OECD and NATO, and collaborates with the EU Network and Information Security Agency (ENISA). A closer collaboration with countries enjoying a more advanced culture of security will also be considered. The *Norwegian Post and Telecommunication Authority* (NPT) participates in the standardisation work in ETSI, and in the ITU. NPT is also a member of the NATO CCPC group, and has frequent contact with sister organisations in Sweden and Denmark. NPT is also represented in the UN WGIG (WG on Internet Governance), GAC/ICANN, and the IRG-SEC.

In the **Slovak Republic**, the Ministry of Transport, Posts and Telecommunications of the Slovak Republic (MDPT SR) closely co-operates with the European Network Information Security Agency (ENISA) to prepare mutual activities.

In **Spain**, the Industry, Tourism and Commerce Ministry co-operates at the international level in the OECD and the EU, especially in the recently founded European Security European Agency (ENISA).

In the **United Kingdom**, most of the players involved in network and information security are engaged with international partners: The National Infrastructure Security Co-ordination Centre (NISCC) plays an active role in the international CERT community and it also interacts with a wide range of other critical national infrastructure (CNI) authorities bilaterally and multilaterally. The United Kingdom also discusses CNI and cybercrime policy and collaboration through the High Tech Crime Subgroup of the G8 Senior Experts' Group on Transnational Organised Crime (the "Lyon Group"). Moreover, there is close collaboration with the United States through an established structure. The United Kingdom is planning to hold a conference as part of its Presidency of the EU and Chairmanship of the G8 to discuss the cross-border issues raised by CNI policy.

The National High Tech Crime Unit (NHTCU) has established effective working relationships with other cybercrime units both in Europe and elsewhere. Their operational activity has led to deployments in over 30 countries across the globe. With support from Foreign and Commonwealth Office funding, the Unit has been able to forge new strategic links through the provision of expertise, equipment and training in 10 key partner countries. In addition, the Unit has accommodated law enforcement experts on attachment from four continents for periods of up to six months to work alongside NHTCU practitioners and learn more of the doctrine of the Unit.

The Department of Trade and Industry (DTI) takes the lead on all discussions internationally where network and information security features as part of a broader economic agenda.[216]

In the **United States**, the National Strategy to Secure Cyberspace foresees the Department of State to lead federal efforts to enhance international cyberspace security co-operation. That leadership and inter-agency co-ordination function occurs in the Department of State's Office of Critical Infrastructure Protection in the Bureau of Political and Military Affairs. The Presidential Decree HSPD-7 reinforces this call, instructing the Department of State in conjunction with DHS and other Departments and agencies to

216. DTI leads in discussions under pillar 1 of the European Union, on UN discussions such as those on Internet governance during the second phase of the World Summit on the Information Society, and on discussions with Asian partners in the ASEM forum.

work with foreign countries and international organisations to strengthen the protection of United States' critical infrastructure and key resources. In addition:

- The National Communications System (NCS) has provided telecommunications sector specific expertise to a number of DHS-led bilateral initiatives in a number of countries.[217] The DHS and the Department of State's (DOS) Bureau of Political-Military Affairs co-ordinates bilateral discussions with other countries, with a focus on Critical Infrastructure Protection (CIP) concerns affecting key sectors. In this context, the NCC provides information on pertinent United States Government policies and procedures, an explanation of operational response and associated priority programmes to the telecommunications sector as well as a thorough appreciation of co-ordination between Government and industry and the objectives a government may wish to consider. The NCS is also an active participant of the North Atlantic Treaty Organisation's Civil Communications Planning Committee (CCPC).[218] Furthermore, the NCS provides a critical link to the emergency response community and the telecommunications companies who provide services to these important telecommunications facilities.
- NIST participates in the International Organisation for Standardisation/ International Electro-technical Commission Joint Technical Committee 1 (ISO/IEC JTC 1) on Information Technology in both Subcommittee 27 (IT Security Techniques) and Subcommittee 37 (Biometrics).
- The Department of Justice regularly participates in various international policy-making bodies that address issues of cybercrime, and has a programme for capacity-building that includes prosecutorial and investigator cybercrime training in various countries. These efforts include seminars on drafting cybercrime legislation, and promoting the Council of Europe's Convention on Cybercrime as a model for legislative drafting on cybercrime.

j) General legal and regulatory arrangements to implement a culture of security

Some respondents listed legal arrangements in their countries, that do not appear in the sub-questions. They are listed below.

Austria lists a number of legal provisions dealing with aspects of IT-security from different legal areas, which define requirements to be met in order to ensure security of automated data processing and networks, in particular on the Internet. These legal provisions include the *Data Protection Act*[219]*, which* contains fundamental guidelines for using data, as well as the *Telecommunications Act,* which also includes provisions on the security of networks,[220] the *Information Security Act*[221] and, based upon this act,

217. Including Canada, Mexico, Germany, the Netherlands, the United Kingdom, Australia, Italy, and Japan.

218. The CCPC, as defined by NATO, is "… responsible for civil communication matters under NATO civil emergency arrangements. Civil communication planning provides for the maintenance of communication services for political, economic and military purposes; in this context the term "civil communications" is seen as telecommunication facilities and services, both public and leased, postal services and any other related services provided by NATO countries, excluding military owned and NATO owned telecommunication facilities." Cf. https://natocep.org. The NCS provides US representation to this group through a resident DOS government representative, and a member of the Telecommunications industry community for specific subject matter expertise.

219. Datenschutzgesetz 2000, BGBl. I Nr. 165/1999 ["BGBl" is for *Bundesgesetzblatt*, best translated as "Federal Law Gazette"], www.ris.bka.gv.at/taWeb-cgi/taWeb?x=d&o=r&v=bgblpdf&d=BGBLPDF&i=593&p=2 ;English version: www.dsk.gv.at/dsg2000e.htm

220. Cf. section 95, Telekommunikationsgesetz 2003, BGBl. I Nr. 70/2003, www.ris.bka.gv.at/taWeb-cgi/taWeb?x=d&o=r&v=bgblpdf&d=BGBLPDF&i=4166&p=62003

the *Austrian Information Security Decree*,[222] which classifies secret information, and determines who is allowed to handle what information.

In 1999 the Austrian Parliament also adopted a *Digital Signature Act.*[223] Together with the *Digital Signature Decree*,[224] the Digital Signature Act determines the legal impacts of digital signatures, conditions for becoming certification authorities (CA) [*Zertifizierungsdiensteanbieter*], guidelines for CAs and their clients, and the supervision of CAs. The *Administrative Signature Decree*[225] determines eased requirements for digital signatures used by the public administration, to have the same legal quality as secure digital signatures in terms of the Digital Signature Act. The E-Government Act[226] establishes the public bodies' duty to publish technical prerequisites under which applications can be filed, and tries to balance the need for data protection and for unique identification in relation to online transactions. Finally, the *FinanzOnline Decree*[227] describes how identification and authentication are to be performed for the Austrian fiscal online portal.[228]

Relevant legislation in the **Czech Republic** includes the Act on Security of the Czech Republic,[229] an Act on the Protection of Classified Information,[230] the Act on Emergency Management[231] the Act on the Integrated Rescue System,[232] the Act on Electronic Signature,[233] the Act on Copyright,[234] the Act on Certain Information Society Services (Anti-Spam Law),[235] and the Act on Electronic Communication.[236]

---

221. Informationssicherheitsgesetz, BGBl. I Nr. 23/2002, www.ris.bka.gv.at/taWeb-cgi/taWeb?x=d&o=r&v=bgblpdf&d=BGBLPDF&i=2717&p=3

222. Informationssicherheitsverordnung, BGBl. II Nr. 548/2003, www.ris.bka.gv.at/taWeb-cgi/taWeb?x=d&o=r&v=bgblpdf&d=BGBLPDF&i=4431&p=

223. The Signaturgesetz, BGBl. I Nr. 190/1999, www.ris.bka.gv.at/taWeb-cgi/taWeb?x=d&o=r&v=bgblpdf&d=BGBLPDF&i=615&p=2 , is based on the European Directive 1999/93/EC on a Community framework for electronic signatures, OJ L 013 , 19/01/2000 pp. 12 – 20.

224. Signaturverordnung, BGBl. II Nr. 30/2000, www.ris.bka.gv.at/taWeb-cgi/taWeb?x=d&o=r&v=bgblpdf&d=BGBLPDF&i=1021&p=3

225. Verwaltungssignaturverordnung, BGBl. II Nr. 159/2004, http://ris1.bka.gv.at/authentic/findbgbl.aspx?name=entwurf&format=html&docid=COO_2026_100_2_72782

226. E-Government-Gesetz (English version): www.cio.gv.at/egovernment/law/E-Gov_Act_endg_engl_Fassung1.pdf).

227. FinanzOnline-Verordnung 2002, BGBl. II Nr. 46/2002, www.ris.bka.gv.at/taWeb-cgi/taWeb?x=d&o=r&v=bgblpdf&d=BGBLPDF&i=2794&p=4

228. Cf. https://finanzonline.bmf.gv.at

229. Act No. 110/1998

230. Act No. 148/1998; cf. www.nbu.cz/en/act148.php

231. Act No. 240/ 2000

232. Act No. 239/2000

233. Act No. 227/2000

234. Act No. 212/2000

235. Act No. 480/2004. The Act on Certain Information Society Services prohibits the dissemination of unsolicited commercial communications ("spam") by electronic means. Dissemination of commercial communications is allowed only with prior consent of the addressee ("opt-in" principle). A fine up to CZK 10 000 000 can be imposed on a legal person or on a self employed person violating the law.

In **Finland**, several laws and regulations contain provisions on information security, including:

The *Act on Openness of Government Activities*, in order to create and realise good practice in information management, stipulates that authorities shall see to the appropriate availability, usability, protection, and integrity of documents, and of information management systems. The Ministry of Finance has issued Government Information Security Instructions based on the Act.

The *Act on Electronic Services and Communication in the Public Sector* (13/2003) contains provisions on rights, duties and responsibilities of authorities and their customers in the context of electronic services and communication. It is aimed at improving the provision of uninterrupted and reliable communication, and to provide for information security in the administration and in the courts, while promoting the use of electronic data transmission.

The *Act on the Protection of Privacy in Electronic Communications* (516/2004) came into force on 1 September 2004. Its objective is to ensure confidentiality and the protection of privacy in electronic communications, and to promote information security in electronic communications.[237] Based on the Act, the Finnish Communications Regulatory Authority (FICORA) has issued *regulations and recommendations* for telecommunication operators.[238]

The *Personal Data Act* (523/1999), the general law on handling personal data, describes the basic level of information security that has to be implemented when processing such data.[239] The Data Protection Ombudsman supervises compliance this Act.[240]

The Act *on Protection of Privacy in the Worklife* (No. 759/2004 of 01.10.2004) sets out the basic rules and rights of the employers, especially regarding the use of e-mail.

Laws on the protection of personal data in **Korea** include the Act on Personal Data Protection in Public Organisations, the Act on Utilisation and Protection of Credit Information, the Protection of Communications Secrets Act, and the Framework Act on Electronic Trades. Other general information security-related laws are, for example, the Electronic Signature Act, the Information and Communication Infrastructure Protection Act, and the Military Secrets Protection Act.

In the **Netherlands**, the Legislation for the electronic highway (1998)[241] has been a starting point for a lot of improvements and adaptations of diverse legislation involving the use of ICT and electronic communication. The protection of private and personal data is covered by the *Data Protection Act,*[242] which came into force in September 2001. The Data Protection Commissioner is the Regulatory Authority supervising the observance of this Act.

---

236. Act No. 127/2005

237. An unofficial English translation of the act is available at: www.mintc.fi/www/sivut/english/tele/telecommunications/Sahk%F6isen_viestinnan_tietosuojalaki_20041213_en.pdf

238. Available in Finnish at www.ficora.fi/suomi/tietoturva/saadokset.htm

239. The Personal Data Act implements the EU Data Protection Directive.

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

241. *Wetgeving voor de Elektronische snelweg* (TK 1998-1999, 25 880 no.1-2)

242. *Wet Bescherming Persoonsgegevens* (Staatsblad, 302, juli 2000).

Additional relevant legislation in **Norway** includes:

- The Security Act with appurtenant regulations, and security classification instructions.
- The Telecommunications Act (Electronic Communications Act) with appurtenant regulations.
- The Act relating to Electronic Signatures.
- Regulations for electronic communication with and within government.
- Security classification instructions (royal decree of 17.3.72, amended 29.6.01).
- The Personal Data Act.
- The Public Administration Act.
- The Freedom of Information Act.
- The Civil Defence Act.
- The civil penal code.
- The Criminal Procedure Act.
- The Police Act.
- Intelligence Service Act.
- The Health Personnel Act.
- Social Security Act.

In **Sweden**, the Electronic Communications Act was expanded in early 2005 to give the National Post and Telecom Agency (the regulator) the powers to initiate actions to increase security and proper functioning of networks to include mobile telephony networks and the Internet. Before, these competences had been restricted to fixed telephony networks. A major Bill on information technology policy is expected to be presented during summer 2005. It is likely to deal with trust in new technologies and to contain a strategy for a secure Internet in Sweden, as well as the government view on the operation of the Swedish top-level domain (.se).

C. Recommendations and other voluntary efforts

Question 3: Has your country developed voluntary, publicly available recommendations to assist government, business and/or users to address the security of information systems and networks? Are such recommendations currently being developed or are there any plans for doing this in the future?

In 2004 **Australia** published the information package *Internet Security for Small Business* to help them address potential security problems. This information package builds upon an existing document *Trusting the Internet* and tackles issues like spam, viruses, e-mail frauds and other online risks. It is composed of two elements:

- A short brochure, which also includes detailed references, aimed at promoting a culture of security for small business, detailing how to manage information security tools or how to address other online risks.

- A booklet detailing the top ten e-security tips.

This initiative has been extensively promoted through industry association channels. Several seminars for small business advisers were organised throughout the country. The material was posted on the security section of the country's Internet Industry Association Web site. In August 2003, an information security portal was developed with the support of the Australian government, bringing together information sources from industry, government and research institutions, to share information and experiences in the field of information security among all stakeholders.

In **Austria**, the Chief Information Officer of the Federal Government has produced a set of information security guidelines, available on its Web site. The Austrian IT Security Handbook helps IT managers within the public administration to develop reliable IT security policies and strategies. The first part of the Handbook addresses IT security management, while the second one tackles areas like organisation, personnel, infrastructure and security technologies. The Handbook was updated and republished in November 2004. Although this publication is mainly targeted at the public administration, the private sector and other actors can also benefit from its insights and guidance.

Austria's Chief Information Officer has also published other more subject-specific operational policy guides that address the Internet, data transfer and e-mail. The objective of the Internet Policy is to put forward common criteria for online communication between public authorities and with external partners. Within this policy, particular attention is paid to information security and the need to develop a standardised approach to foster secure information exchanges. Along the same lines as the Internet Policy, the E-mail Policy defines general principles, requirements and recommendations for e-mail exchanges. It examines issues like identification, authentication and confidentiality of information, with a focus on security issues associated with electronic signatures and encryption. The Transfer Policy addresses the security of data exchanges between organisations. In the future, the CIO's office is also expected to publish a Domain Policy.

Industry **Canada** has been actively promoting the OECD Security Guidelines within the public and private sector, and has taken a variety of additional specific initiatives related to information security. Recently, it has issued *The Principles for Electronic Authentication*, providing guidance in handling functions and overall responsibilities in the authentication domain. The principles, in particular, identify essential elements of security, privacy, disclosure and complaint handling to be addressed when designing, developing, implementing and assessing an authentication service.

Since their launch, Industry Canada has been working on promoting the incorporation of the authentication principles in industry codes, guidelines and other private sector initiatives. Building upon this experience, they will address the security complexities associated with the management of digital identities.

In **Denmark**, the government regularly publishes and distributes IT-security related documents and guidelines. Currently, it is focusing on developing best practices and other guides for the implementation of digital signatures within the private and public sectors.

In **Finland**, several public actors are involved in developing and disseminating information security-related recommendations. The Finnish Communication Regulatory Authority (FICORA) publishes recommendations for telecommunication operators. However, these documents are also useful to other business sectors in managing information security. CERT-FI, distributes information security advisories through the Web, e-mail and text-TV. Moreover, it maintains two Web sites to support the strategic objectives of the country's regular national information security day. One of these sites is targeted to end-users in general, the second to students.

Finland's Ministry of Finance has also published instructions and recommendations for government institutions, covering all areas of information security. In particular, in 2004 the Ministry issued the recommendation *Information Security and Management by Performance* that provides principles on how to develop information security policies and management performance measurements. The text makes direct reference to the principles of the OECD guidelines. This recommendation builds on other information security-related documents like *The Assessment of Information Security Management* and *The Risk Assessment Instruction to Promote Government Information Security*, which provide guidance on how

to evaluate the level of security preparedness of organisation and possible future courses of action. While developed for government institutions, the recommendations can also be used by the private sector.

The Ministry of Interior has set up an Advisory Committee on Information Management in the Public Administration to promote co-operation in information management between the central State and the municipalities. This body is primarily responsible for making reports, undertaking studies and drawing up recommendations. Although security is not the primary focus, it is seen as a key element for the success of related information exchanges and for service interoperability.

France uses the principles of the OECD guidelines to raise awareness and provide guidance for information security. The Central Directorate for Information Systems Security (DCSSI) has recently issued a guide for the development of information security policies and risk management methodologies. It is also working with the ADAE (*Agence pour le Développement de l'Administration Electronique*) for the application of general information security principles through a new policy called PRIS[243] that defines security requirements applicable to trust service providers and security products used for secure access to public e-services. PRIS is organised around three security levels and several security functions like electronic signature, authentication, confidentiality, and time-stamping.

Germany's Federal Office of Information Security develops and offers information and guidance for both professional users and citizens through its Web site. Among its many publications are the IT Baseline Protection Manual, Baseline Protection Tools and Guidelines and Secure Use of Telecommunication Equipment. BSI also produces several brochures and information material examining the security implications of topics like wireless, GSM, Bluetooth, as well as studies on a wide-ranging set of technologies such as biometrics, RFID and Web applications. In 2003, the office also launched a specific Web portal aimed at private PC users. Through the site, citizens can also sign up to a newsletter with up-to-date information about risks, and on more general aspects of information security.

Finally, the Federal Ministry of Economics and Labour and the Federal Ministry of Interior have launched a Web site targeted at SMEs, with information on secure Internet and e-mail use, and check-lists. With support from the Government, TeleTrusT Deutschland e.V. has published a brochure called *IT Security Made in Germany-Best Practice in Secure Business Processes*. It was presented in September 2004 during the annual Information Security Solutions Europe (ISSE) conference, a leading European information security event. The document is primarily targeted to experts in the encryption and information security domains and provides an overview of the state of the art of information security in Germany.

In **Japan**, the Ministry of Economics, Trade and Industry (METI) undertakes several activities in the field of information security. In April 2003, it issued a notice addressing information security auditing and management. In September 2004, a Committee for Information Security Governance was established to discuss the issue of security benchmarks. Previous initiatives of the same ministry include the publication of Computer Virus Prevention Guidelines to tackle the spreading of malicious software (1996), and a similar initiative regarding the prevention of unauthorised computer access (1996).

In 2000, the country's IT Security Promotion Committee in the Prime Minister's office issued a set of guidelines for IT security policies, directed at government ministries and agencies. Already in September 1997, the National Policy Agency had issued specific guidelines on information security and cyber-crime.

In **Korea**, a *Cyber security Manual* has been developed to assist both individual and business users such as employees, system operators, managers of Internet cafes and service providers. It is available both on CD and on line. By the end of 2004, over 10 000 copies had been distributed. Moreover, a booklet and

243. www.adae.gouv.fr/article.php3?id_article=547

mouse-pads with *Information Security Practice Guidance* have been prepared, with eight practical measures for general users to protect themselves from cyberrisks.

Korea also uses different channels to distribute information. It operates a security instant messenger where security-related information is distributed in real-time, and the Sec-Info mailing list which distributes relevant security information. The government has also co-operated with security companies to organise a monthly Hacking and Virus Prevention day. During the event, participants can download antivirus software for free. During the second half of 2005, the Ministry of Information and Communication (MIC) plans to classify the small and medium sized enterprises based on each company's IT assets and budgets, and will develop information security guidelines specific to each class. In addition, the MIC will produce and distribute booklets and promotional movies to help those companies respond effectively to the new variety of threats, for example phishing and spyware.

In the **Netherlands**, the Ministry of Economic Affairs is responsible for initiatives aimed at assisting government, businesses and users about information security issues. The *Kwetsbaarheid op Internet* (KWINT) programme has launched several initiatives developed through public-private partnerships between government, industry, consumer organisations and experts. First, a brochure entitled *A Safer Internet for All* provided an overview of the main information security issues. In 2003, the report *Monitoring Internet Safety* provided an overview of risk assessment inside companies. In 2004, an information security guide targeted at SMEs was completed, and a guide to managing cyberincidents.

The Ministry of Economics has also launched the *Surf of Safe* campaign aimed at raising public awareness about information security. The campaign targets a broad group of private users (including children and parents) and SMEs. As part of this campaign, several brochures were prepared and widely distributed to all households. The Ministry also partnered with the Foundation "ICT at School", with Kennisnet and the Consumer Organisation for Children in a campaign to inform children and their parents about responsible use of the Internet. Finally, the Ministry of Economics is running an alert service distributing information through the Web, mailing lists and SMS. Moreover, through this organisation's Web site, it is possible to access specific security issues and incident reports on line.

GOVCERT.NL has produced the manual *From Recognition Towards Declaration* to assist organisations in dealing with cybercrime. This publication was prepared in partnership with the national police, the Ministry of Justice, the Dutch Forensic Institute and the association of service providers. It is targeted at managers and lawyers.

The National Platform Crime Control has partnered with ECP.NL, a public-private partnership, to provide information about security to small and large companies. Their Web site provides a list of security firms and security products.

In **Portugal**, the government is planning to develop a set of security guidelines, *e.g.* for PCs at home or at work. Particular attention will be directed to providing guidance for risk management.

In **Spain**, the General Direction of Information Society has provided support for repetitive campaigns to foster information security awareness. These activities have been organised and co-ordinated with industry, using the Internet and other means to distribute information about information security and risks. In particular, as part of the Network Security Campaign, a specific Web site was created with general information about information security.

In **Sweden**, the Swedish Emergency Management Agency (SEMA) is producing recommendations for baseline security. The defined level establishes a minimum level of security for IT-systems necessary

for essential social activity. These recommendations apply to both public and private entities.[244] In order to implement the baseline security SEMA has produced an IT security guide as an instrument for analysis of the security of IT systems. SEMA is also producing a monthly newsletter (Delete) in order to raise awareness for information assurance, and has published a DVD-film (Be-Aware) containing interviews with managing directors within the Swedish society about ideas and best practices concerning the responsibility for the IT-security within organisations, to raise awareness at management level. The SEMA products are disseminated through predefined mailing lists, through SEMA's Web site, a monthly newsletter, and through various other networks. The Swedish Agency for Public Management (*Statskontoret*)[245] has published guidance to implement the international and Swedish standard ISO/IEC17799.[246]

The National Post and Telecom Agency[247] has published information on Internet security for citizens and SMEs, based on their own expertise and public consultation.[248] The Swedish IT Incident Centre (Sitic)[249] contributes to this work, and also publishes information and advice in their specific area of activity. The material is mainly made available on Web sites, but also in print and on promotional cards. Representatives of the agencies also appear at conferences and courses.

Short and general information is available from the Swedish Consumer Agency.[250] This is mainly advice and recommendations about rights of consumers when shopping on the Internet and how to avoid problems while surfing or shopping on the Internet.[251]

In the **United Kingdom**, the Cabinet Office has in conjunction with the National Technical Authority for Information Assurance (CESG) and the National Infrastructure Security Co-ordination Centre (NISCC) issued guidance for government departments. The Central Sponsor for Information Assurance (CSIA) has sought to establish Board ownership of the information security issue within Departments so that there is one senior responsible officer. The CSIA has the role of accrediting cross-departmental systems to ensure that they meet certain requirements, and has produced security framework documents to enable secure transactions between government and the private sector. The government also promotes the importance of treating information security as a key business issue: The Department of Trade and Industry (DTI), the National High Tech Crime Unit (NHTCU) and the CSIA have produced guidance material aimed at business and home users. For home users this guidance is basic computer hygiene, for smaller businesses, it is based on the concept of risk management and the selection of appropriate controls. The guidance follows the structure of the OECD guidelines. In addition, Part 2 of the British national BS 7799 standard has an annex which indicates the relation between the standard and the guidelines.

244. www.krisberedskapsmyndigheten.se/2060.epibrw

245. www.statskontoret.se/default____309.aspx

246. The guide, named OffLIS (available at www.statskontoret.se/offlis), consists of guidelines and templates to issue information security policy documents. Furthermore it gives guidance for an organisation's process for information security management from classification of information assets, support to communicate policy statements, to audit for information security within systems and/or organisational parts.

247. www.pts.se/Default.asp?Sectionid=&Itemid=&Languageid=EN

248. www.pts.se/Internetsakerhet/

249. Sitic: www.sitic.se/eng/index.html

250. www.konsumentverket.se

251. Such as advice on e-commerce, secure surfing, unsolicited e-mail marketing (spam). A part of this has been driven by the agency's experience of the problem of hijacked computer modems. Cf. www.konsumentverket.se/mallar/en/lista_artiklar.asp?lngCategoryId=922

In the **United States**, several government organisations are involved in disseminating voluntary guidance to businesses, citizens and other members of civil society. The Department of Homeland Security (DHS)'s National Computer Security Division (NCSD) distributes relevant and current information on information security issues through the US-CERT. Interactive forms are provided for reporting cyber incidents. The National Cyber Alert System (NCAS) provides registered users with detailed and up-to-date information about cyber security risks and vulnerabilities. Since its launch in 2004, over 270 000 have registered with the system to receive regular alerts and updates. NCSD is also engaging industry and academia through the National Cyber Security Partnership to foster a common understanding of information risks, and possible solutions and responses.

The National Security Telecommunication Advisory Committee (NSTAC) provides the US President with industry based analysis and recommendations on a wide range of policy and technical issues in the field of information and communication technologies. NSTACs *Next Generation Task Force* is currently developing new cyber-risk scenarios to determine future technical and operational requirements. An interim report of their activities is expected for mid-2005. The *National Infrastructure Advisory Council*, composed of 30 members from government, industry and academia selected by the US President has since its establishment in 2001 developed reports and best practices in the areas of critical infrastructure protection, interdependencies and overall vulnerability assessment.

The National Institute for Standards and Technology (NIST) also provides voluntary recommendations and guidance on information security. According to the Federal Information Security Management Act of 2002, NIST is tasked with developing standards, guidelines and associated methods and techniques to assist government departments in providing adequate protection for their systems. The guidelines tackle issues like cryptography, certification, risk management, contingency planning, intrusion detection and general issues of information security management. NIST documents are freely available from its Web site, which received about 26 million hits in 2004. NIST is also co-operating with the US Small Business Administration, the Federal Bureau of Investigation (FBI), the US Chamber of Commerce and the National Cyber Security Alliance on fostering information security awareness among small and medium-sized enterprises.

The Federal Trade Commission, following the revision of the OECD *Guidelines*, has launched a multifaceted information security awareness campaign targeted at children, consumers and businesses. At the core of this campaign is a Web site where individuals can access plain language guidance on how to stay safe on line, and select appropriate security solutions to respond to viruses and other risks. The FTC has distributed publications, and prepared newspaper articles and video news releases. The Commission has also directed attention to raising information security awareness among lawmakers, and has organised several public workshops examining complex issues like spyware, spam, RFIDs and peer-to-peer communications.

The **Czech Republic** has indicated that recommendations will be developed after the approval of the country's National Information Security Strategy. The **Slovak Republic** has no initiatives in this domain.

II. Government as owner and operator of systems and networks

Question 4: Action taken to develop a culture of security within the government itself (distinct government plan; measures taken in each of the possible areas of government action related to its role as owner and operator of systems and networks to develop a culture of security)[252]

In **Australia**, the E-Security National Agenda, announced in September 2001, forms the *e-security policy framework* for protecting the national information infrastructure. Initiated by the Agenda, the E-Security Co-ordination Group (ECSG) is the core **policy** *development and co-ordination body* on e-security matters. Its objective is to develop a secure and trustworthy electronic operating environment for both the public and private sectors. It is comprised of various law enforcement and security agencies. The government signed an agreement with the Australian Computer and Emergency Response Team (AusCERT) to create a national *Information Technology Security Reporting and Alert Scheme* which allows computer users to receive alerts about common threats and report suspected incidents.

In addition, Australia is leading *international action in the APEC region to build CERT capacity* (CERT Project), raise awareness of the value of CERTs in developing economies and establish a network of CERTs throughout the Asia-Pacific region.[253] The CERT project helps develop guidelines for establishing CERTs and provides funding for a CERT communications network at the regional level. Australia is also overseeing an APEC-funded project for in-country CERT training.[254]

The **Austrian** Information Security Act[255] provides that each federal ministry has to appoint a security officer responsible for IT security within the ministry, and that each administrative unit has to adopt an IT security policy. All ministries have been urged to submit a plan for the implementation of their security policies by March 2005 and a working group of security officers will compare them and allow for cross-ministry discussions and information exchanges. Secure mobile access to government resources and applications will be a specific topic for the 2006 Austrian presidency of the EU and, to this end, standard tools for notebooks are being developed. The citizen card already enables the use of file encryption with Microsoft operating systems and the creation of signed reports with Microsoft Word. Other initiatives include: sample implementations for electronic payment; a reference for calculating sector-specific personal identifiers in different programming languages; and a service ("testmail") to check whether e-mail systems are compatible with the e-mail policy. In addition, the largest electronic data processing centre for the federal government[256] is currently finalising its security certification (ÖNorm A 7799, based on ISO 17799).

The Austrian IT Security Handbook also contributes to the creation of a standard approach. Internet policies provide minimal requirements and best practices as well as Security Levels[257] and Security Classes[258] in the Portal Group. As regards electronic transactions with the administration, the

252. Question 4 was primarily related to the operation-oriented principles (6-9) of the 2002 OECD *Security Guidelines*.

253. In Papua New Guinea, the Philippines, Thailand, Vietnam, and Indonesia.

254. In Chile, Mexico, Peru, and Russia.

255. Informationssicherheitsgesetz, BGBl. I Nr. 23/2002, www.ris.bka.gv.at/taWeb-cgi/taWeb?x=d&o=r&v=bgblpdf&d=BGBLPDF&i=2717&p=3

256. www.brz.gv.at

257. *Sicherheitsstufen für die Kommunikation Bürger–Behörde im Bereich e-Government*, www.cio.gv.at/securenetworks/si-stu/sicherheitsstufen_v13_20030724.pdf

258. http://reference.e-government.gv.at/Sicherheitsklassen.329.0.html

"administrative signature" will during a transitional period be regarded as equivalent to a secure signature in the context of citizen-card applications, and will allow for unrestricted and secure access to e-government. The "official signature", used by public authorities, will also allow citizens and businesses to verify the origin and integrity of a given electronic administrative document. Insecure password systems and separate registration for each application will be replaced by the electronic signature step by step. The modules for online applications (MOA),[259] the citizen card and the security layer for administrations to access the card are also important building blocks for the creation of secure e-government applications.

In **Canada**, federal departments and agencies have to apply the Government Security Policy[260] which requires them to have an IT security strategy. The Policy on Management of Government Information[261] requires that departments protect information throughout its lifecycle. The Treasury Board Secretariat (TBS) is responsible for co-ordination, leadership, oversight and monitoring of the policy. TBS' role encompasses various functions including the development and update of the policy; the development of technical standards and documentation; training; advice and assistance; awareness raising; research and development; recruitment and representation in national and international committees. Four other bodies also have responsibilities for co-ordinating information security activities: Public Safety and Emergency Preparedness Canada (PSEPC), the Canadian Security Intelligence Service (CSIS), the Communication Security Establishment (CSE), and the Royal Canadian Mounted Police (RCMP).

As regards specific initiatives, the Management of Information Technology Security (MITS) standard, developed by the TBS, sets baseline security requirements for federal departments, including management controls, risk assessments, dealing with security incidents and weaknesses in systems, auditing security, and business continuity planning. MITS provides an overall framework for including IT Security risks in a corporate risk profile. Canada also reports the existence of a protected Web-based forum allowing departments to share information and experience. A government-wide plan will be developed by the TBS to identify priorities for the development of further standards.

The effectiveness of the policy will be assessed by TBS in a mid-term report based on internal audits and active monitoring of the programmes departments are required to undertake. The MITS standard requires departments to conduct annual reviews of IT security based on a self-assessment tool developed by the TBS. A government-wide self-assessment was completed in April 2004. In addition, departments are required to conduct regular technical vulnerability assessments. The Auditor General of Canada conducted government-wide IT security audits in 2002 and 2005. The 2005 report stressed the need for improving oversight and monitoring. The Government plans to fully implement the MITS standard by December 2006. The initial priority is to establish fundamental and efficient security processes and organisation required to effectively manage IT security risks in the departments. Other priorities are under review, including senior management awareness and understanding of security risks.

As regards response, Canada established the Canadian Cyber Incident Response Centre (CanCERT). It is developing a new security incident management standard, and the architecture for an integrated government-wide incident detection and response capability. Finally, as regards the protection of critical infrastructure, departments are required to maintain an inventory of critical systems and services. The Business Continuity Planning (BCP) standard requires departments to complete BCPs for all their critical systems.

259. Cf. Question 8g) below.

260. www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp

261. www.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_GIH/mgih-grdg_e.asp

The **Czech Republic** will plan specific initiatives after the approval of the National Information Security Strategy. The creation of a body to co-ordinate information security activities is expected.

In **Denmark**, the Ministry of Science, Technology and Innovation is responsible for the implementation of security of information systems and networks in the public sector. The IT security division in the National IT and Telecom Agency develops and co-ordinates related activities. Institutions in the government are required to implement an IT security standard based on a national implementation of the ISO/IEC 17799 standard (DS 484). The Ministry has made the standard available to all governmental organisations free of charge. Several initiatives have been taken: a programme to help institutions implement the standard; guidelines; an Internet portal with information about the standard and its implementation; workshops and a 12-step implementation course to guide users. In addition, a working group was created. The implementation of the standard is measured on an annual basis.

In **Finland**, a broad set of instructions has been released by the Ministry of Finance, including the protection of critical Government information systems, risk assessment, secure IT architecture for remote access, authentication in government services, information security for remote work, recommendations for ICT rooms, and checklists for ICT procurement and for outsourcing. Several initiatives have been taken, for example on spam, e-mail certificates and critical infrastructure.

In **France**, the "State Information System Security Reinforcement Plan" 2004-2007 covers public systems and networks. Upon notice, the Expert Government Response Centre for the Treatment of IT Attacks (CERTA) provides support to agencies in tackling incidents. The Central Directorate for Information Systems Security (DCSSI) provides consulting, audit and training to public bodies.

In **Germany**, the federal government's central communication infrastructure (Berlin-Bonn Information Network, IVBB[262]) which connects 45 000 workplaces, the Federal Administration Information Network (IVBV - the federal government's intranet) and "TESTA Deutschland" (connecting the federal and the federal-states administrations' networks) are based on an encrypted, firewall-protected and permanently monitored and checked infrastructure. The Federal Office for Information Security oversees security in the German part of the European TESTA network for government administrations recently joined by the country. The "E-Government Manual",[263] designed by the Federal Office for Information Security and the Federal Ministry of the Interior, is the basic security document of the e-Government initiative (BundOnline 2005).[264] It includes the "Standards and Architectures for E-Government Applications – SAGA".[265]

The Federal Office for Information Security has developed SINA[266] (Secure Inter-Network Architecture), a client-server application to process highly confidential (including top secret) information in insecure networks. It has also carried out a series of PKI interoperability tests of e-mail products (Sphinx project),[267] and a project to develop secure e-mail open source interoperable software (Ägypten 1/2).[268]

---

262. www.kbst.bund.de

263. www.bsi.bund.de/fachthem/egov/3_en.htm (English)

264. www.bundonline2005.de

265. www.kbst.bund.de/Anlage304417/Saga_2_0_en_final.pdf (English).

266. www.bsi.de/fachthem/sina/index.htm (German), www.bsi.de/fachthem/sina/download/downloads.htm (German/English).

267. www.bsi.de/fachthem/verwpki/sphinx/index.htm (German).

268 www.bsi.de/fachthem/verwpki/aegypten/index.htm, www.gnupg.org/aegypten/index.de.html

German federal authorities can use the CERT-Bund[269] services for prevention and response purposes. CERT-Bund is available 24/7, provides information on vulnerabilities, issues warnings, receives incident reports and provides recommendations. It is a member of the *CERT-Verbund* (German security and computer contingency teams), of the European Government CERT (EGC) group, and of the Forum of Incident Response and Security Teams (FIRST).

Germany also reports activities on protection against bugging, critical infrastructures, and penetration tests. In particular, Germany co-hosted with the United States the International Watch, Warning and Incident Response (IWWN) Workshop in Berlin in October 2004. Further national and international projects are planned for 2005. The IT penetration centre of the Federal Office for Information Security currently focuses on checking the security of Internet applications for the BundOnline 2005 initiative, on auditing the Berlin-Bonn Information Network, and on managing defence against attacks by Trojan horse programs.

In **Japan**, an "Action Plan for Ensuring e-Government's IT Security" was adopted in 2001 by a committee chaired by the Deputy Chief Cabinet Secretariat, composed of all ministries and agencies. The "National Information Security Center", established in December 2004 in the Cabinet Secretariat,[270] is responsible for planning and co-ordinating the promotion of IT security in the public and private sectors.

The National Incident Response Team (NIRT),[271] created in 2002 in the IT Security Office of the Cabinet Secretariat, alerts ministries and agencies on incidents, develops technical countermeasures and assists in implementing countermeasures. In addition, the "Cyber Force" of the National Police Agency, a mobile unit present in each regional police bureau, provides technical assistance and analysis to prevent and mitigate damages, and to make arrests in case of cyber terrorism on a 24/7 basis. NIRT, the IT Security Office and Cyber Force co-operate and interact. Co-operation with other stakeholders includes communication with the media to alert the public if an incident is expected to have impact on people's lives.

In 2002, the Cabinet Secretariat evaluated the implementation level of the IT security policy (2000) in ministries and agencies. As a result, the "Guidelines for IT Security Policy" and the IT security policies of ministries and agencies were revised. IT product procurement for the Japanese government should be ISO 15408 certified, when possible.

In **Korea**, each ministry has introduced a patch management system. As regards security warnings, a shared information system has been created to facilitate co-operation among government agencies. Information security activities of national and public organisations are mainly divided into information security system monitoring, information system security measure support, information security product evaluation, security training, and urgent response to cyber terrorism. The Korean Government is operating a 'National Information Security Management Team' and a 'National Security Research Institute' under the umbrella of the 'National Intelligence Service' to protect critical information and to evaluate the information security products, respectively. It has also established a National Security Monitoring System managed and operated by the National Cyber Security Center. In 2003, the Ministry for Information and Communication (MIC) provided information security systems and consulting services to 44 central administrative agencies and 16 local organisations. In addition, MIC has been offering information security education services to the employees of the government and of public organisations.

---

269. www.bsi.de/certbund/index.htm, www.cert-verbund.de (German), www.bsi.bund.de/certbund/EGC/index_en.htm (English), www.first.org (English).

270. The National Information Security Center replaces the former IT security office established in 2000.

271. www.bits.go.jp/en/sisaku/h1403nirt.html

In the **Netherlands**, the Innovation and Information Policy Department of the Ministry for the Interior and Kingdom Relations is responsible for information security co-ordination. The "Directive on Information Security for Central Government" requires ministries to establish information security measures. The Directive incorporates principles of the OECD *Security Guidelines*: The risk assessment principle, for example, is reflected in the dependency and vulnerability analysis foreseen in the Directive. The departmental accounting services and the Netherlands Court of Audit are responsible for supervision of compliance.

The Dutch government applies a Code of practice for information security management, compatible with the ISO/IEC 17799 standard. A project for a secure emergency communication network (C2000) between the police, fire brigades, ambulances and the military police came into operation in 2004. More and more emergency service providers are using C2000 which is under the responsibility of the Ministry of the Interior and Kingdom Relations. The same ministry also launched a PKI programme[272] to enable secure communication with and within the government (e-mail security, digital signature of formal documents, contracts and electronic documents, desktop security, safe access wireless networks, secure Internet/Intranet). Finally, GOVCERT.NL[273] prevents and handles incidents for national, regional and local government institutions and agencies. Besides watch and warning activities, GOVCERT.NL organises workshops, conferences and other events to exchange knowledge and experience, and participates in national and international co-operation and information sharing. Its yearly budget is EUR 2 million.

In **Norway** each sector and government entity has developed plans and taken action for security, based on a risk analysis. A monitoring service for co-ordinated incident detection and warning has been put in place (VDI service). Following up on the national strategy on information security, an action plan is under development with advice on relevant security measures resulting from risk assessment and on a review of existing regulations and other legal issues.

Portugal is in the process of developing a National information security framework which is not expected to distinguish between the public and private sectors.

The **Slovak** Ministry of Transport, Posts and Telecommunications will in the future co-ordinate the Governments' information security activities. It already now co-operates closely with the European agency ENISA. Once the new act is adopted, government systems security will be subject to security standards. The establishment of a CSIRT institution is planned in the near future (2005-2006).

In **Spain**, the Public Administration State Secretariat mandated the implementation of information security policies within government departments in May 2004.

In **Sweden**, issues of developing a culture of security within the government are currently being analysed by the Commission on Information Security that will deliver its final report in September 2005. The deliberations in the Commission include a wide spectrum of activities from regulation to research and training programmes. The Swedish Emergency Management Agency (SEMA) is responsible for overseeing national information assurance in Sweden, and hosts various forums in order to develop a common culture of information assurance.[274]

---

272. www.pkioverheid.nl

273. www.govcert.nl

274. There are forums solely for the private sector, forums solely for the public sector and there are also forums for both the public and private sector (public private partnership - PPP). The purpose of the forums is to create coherent and strong efforts within the area.

As regards co-ordination with other stakeholders on vulnerability discovery, disclosure and patch management, the Swedish IT Incident Centre has been established with government organisations as part of its constituency in its CERT/CSIRT tasks, and works on watch and warning, as well as incident report handling. The organisation provides security / vulnerability information for all government agencies to make use of. It also handles vulnerability disclosure, globally co-ordinated when required. The Swedish IT Incident Centre also provides information and training to government agencies on CSIRT related matters. The Swedish Agency for Public Management also provides support in this field. Finally, the Defence Radio Establishment supports government agencies and state owned companies with technical competence and penetration testing.[275]

In the **United Kingdom**, the government's responsibility to secure its own systems is part of its overarching information strategy to make sure that information is available when it is needed. This strategy has created a central role for the Central Sponsor for Information Assurance (CSIA).[276] The CSIA has asked government departments to appoint a Senior Responsible Officer – preferably at Board level, and works with the National Technical Authority for Information Assurance (CESG) to ensure that solutions and guidance are available to help government departments handle risk management processes. All government departments use the ISO 17799 standard and several departments have certificates of compliance with BS 7799 part 2. The CSIA also undertakes a system of accreditation to ensure that systems meet the standards expected and there are regular surveys to ensure that government departments are applying the advice which has been issued. Real time alerts and warnings are provided by the government CERT (Uniras) which is under the management of the National Infrastructure Security Co-ordination Centre (NISCC). Uniras works in collaboration with the community of CERTS within the United Kingdom and with other CERTS elsewhere. Alerts and warnings are issued to all government departments and the management of the Critical National Infrastructure (CNI). Such information is also increasingly being filtered and passed down to less technically literate users through the ITsafe service and the expanding network of the Warning Advice and Reporting Points (WARPs).

In the **United States**, the 2002 E-Government Act[277] recognises the importance of information security to the economic and national security interests of the country and aims to foster a culture of security within the Federal Government, in particular at the level of Federal Agency Directors. The development of standards, policies and regulations rests with the National Security Agency (NSA) for national security systems, and the National Institute of Standards and Technology (NIST) for other systems. The Federal Information Security Management Act of 2002 (FISMA) and the US Office of Management and Budget (OMB) security policies[278] require security assessment and a continuing cycle of risk assessment for all federal agencies. FISMA provides a framework for enhancing information security in the federal government.[279] NIST has developed a set of security standards and guidelines, for example security categorisation standards, and standards and guidelines for the specification, selection and testing of security controls for information systems.

Several communication and collaboration initiatives also foster enhancing information security in the public sector. Four groups have been created to exchange information, share experience and discuss specific topics: *i*) The Chief Information Security Officers Forum (CISO Forum) created by the National Cyber Security Division (NCSD) meets quarterly and holds separate working group meetings on an as-

275. www.fra.se/english.shtml

276. Cf. question 1 above.

277. PL 107-347, December 2002.

278. OMB Circular No A-130, Appendix III, "Security of Federal Automated Information Resources".

279. Guidance for FISMA requirements is available at www.whitehouse.gov/omb/memoranda/m03-19.pdf

needed basis; *ii*) Inside the US-CERT, the Government Forum of Incident Response and Security Teams (GFIRST) is a community of federal agency emergency response teams where technical and tactical practitioners of security response teams can meet; *iii*) The Federal Computer Security Program Manager's Forum, hosted by NIST, is an informal group of over 500 members. It helps NIST exchange information directly with the people in charge of addressing information security issues in the federal government; *iv*) The Information Security and Privacy Advisory Board is a federal advisory committee that brings together senior professionals from industry, government and academia to help advise NIST, OMB, the Secretary of Commerce, and US Congress about information security and privacy for unclassified federal information systems.

Question 5: Information and/or statistics collected on the budget for security of information systems and networks in the public sector. Targets set for the proportion of information security spending in the public sector. Plans for such or similar measures for the future[280]

Australia has allocated EUR 14.806 million[281] (AUD 24.9 million) over four years for national information infrastructure protection, including building infrastructure and awareness raising.

In **Canada**, the Treasury Board Secretariat gathers reports from departments on security spending and budgets to improve the overall financial management, ensure alignment with government priorities and identify possible efficiencies. The Government has no plans to set targets for IT security spending. The target level of IT security spending is established by each department's senior management as part of the overall corporate risk management. However, the Treasury Board Secretariat will establish target levels for investment in common security infrastructure and services to improve government-wide efficiency.

Denmark does not collect information on IT security budgets. However, based on estimations from *Dansk Industri*, the Meta Group, the Gartner Group and others, the Ministry of Science, Technology and Innovation suggests that information security spending amounts to approximately 10% of the IT budget.

In **France**, no statistics are available on the budget for security of information systems and networks which is apportioned amongst Ministries to finance their activities, and the Central Directorate for Information Systems Security (DCSSI). However, the budget for the State Information System Security Reinforcement Plan, covering the period 2004-2007, is estimated at EUR 180 million.

In **Germany**, internal statistics on expenditure by the federal government on IT security show that expenditure rose almost 100% between 2001 and 2004. The budget of the Federal Office for Information Security (BSI) increased by around 50% during the same period, and many new IT security specialists were recruited. Expenditure on IT security in Germany will continue to increase in 2005.

In **Korea**, the Ministry of Information and Communication (MIC) has conducted a survey on the information security budget in relation to overall IT spending in the government sector in August 2004. Questionnaires were sent out to each of the 59 central government organisations' divisions in charge of information technology or information security, followed by phone calls to explain the objective and content of the survey. The survey showed that the ratio of the security budget on the overall IT budget rose from 2.77% in 2003 to 3.31% in 2004. The survey will be repeated annually. Korea suggested to the WPISP in October 2004 the adoption of an OECD indicator of information security spending to allow for comparison among OECD member countries. The Korea Information Security Agency (KISA) conducts annual surveys on information security with private enterprises and individual Internet users on the current

280. This question was primarily related to the policy-oriented principles (1-5) of the 2002 *OECD Security Guidelines*.

281. Currencies are converted in Euros according to the exchange rate of 7 April 2005.

state of the 'level of security awareness', the 'use of security products', 'PC security management', etc. The Korea Internet Security Center (KISC), a subsidiary of KISA, posts monthly hacking and virus statistics on its Web site.[282]

In the **United States**, the Office of Management and Budget[283] (OMB) is responsible for gathering statistics on the budget for security of information systems and networks. The General Accountability Office[284] (GAO) also produces reports with additional statistics.

Austria, the **Czech Republic**, **Finland**, the **Netherlands,** the **Slovak Republic** and the **United Kingdom** do not collect such information.

Japan, Norway, Portugal and **Spain** gave no answer to this question.

III. Government as user of information systems[285]

Question 6: Most effective programmes and initiatives to develop a culture of security among users of government systems

As part of **Australia's** E-Security National Agenda, the government has created an E-Security Co-ordination Group. This group provides the country's core policy for development and co-ordination on e-security matters and has the strategic goal of developing a secure and trusted electronic operating environment for both the public and private sectors.

In **Austria**, the security guidelines of the federal government for the electronic delivery of data foster a culture of security with the users of the public sector systems. The "citizen card" is also expected to foster a culture of security among citizens through highlighting the importance of protecting the security of their data, and to increase the understanding of wireless security issues, as the "citizen card" is available on mobile phones. Austrian mobile operators and the Chief Information Officers of the federal government are co-operating on this issue.

Industry **Canada** has been managing several initiatives aimed at small and medium-sized enterprises, including the Canadian e-Business Initiative, which involved the organisation of several seminars and the preparation of tailored Web sites, information packages and assessment tools. An example of these activities is "PrivacyForBusiness", a Web site specifically aimed at promoting the country's Personal Information Protection and Electronic Document Act (PIPEDA). The site provides a one-stop shop where organisations are offered guidance on how to be compliant with this legislation. Another example is the site "E-biz.enable". It is a comprehensive online resource that allows SMEs to explore e-business problems and solutions relevant to their company and their success in the global online environment.

In **Denmark**, not all government institutions have completed the implementation of the IT security standard DS 484 as yet. However, it can already be seen that more resources have been allocated to tackle information security topics and issues.

282. www.krcert.or.kr

283. www.whitehouse.gov/omb

284. www.gao.gov

285. Question 6 was primarily related to the operation-oriented principles (6-9) of the 2002 *OECD Security Guidelines.*

In **Finland**, the government is playing a significant role in fostering a culture of security for users of public sector systems through its *Government Information Security Development Programme.* It has 28 initiatives involving about 300 people and plenty of organisations from all administrative sectors to address topics such as performance management and metrics of information security, international co-operation, legal compliance and end user security. The Ministry of Finance summarises the approaches and development of these projects in its VAHTI 1/2004 document, which is freely available on line.

In **France**, the development of the EBIOS risk assessment and management methodology (*Expression des Besoins et Identification des Objectifs de Securité*) and the associated exchange of best practices has played a significant role in fostering security awareness with public sector organisations. In 2005 about 100 EBIOS exercises are expected to be performed on new e-services established by the French public administration. Moreover, CFSSI (the DCSSI training centre) is currently contributing to creating awareness by holding different courses on information security.

In **Germany**, the government is playing an important role in fostering a culture of security among government officials, building upon e-government initiatives. As part of the Bund Online 2005 programme, several initiatives have been launched such as the virtual post office. Fostering security is an important element within these initiatives. The awareness raising activities of the Federal Office for Information Security (BSI) among government officials are of particular importance in this context. The German Federal Ministry of Economy and Labour (BMWA) has since 1999 supported the development, harmonisation and transfer of secure e-government solutions through the R&D programme MEDIA@Komm and its successor MEDIA@Komm-Transfer,[286] where security, reliability and trust in communication and transaction services between administrations, business and citizens have been addressed as key issues. MEDIA@Komm has developed numerous best-practice solutions for integrated platforms and services covering all facets of e-government and has delivered field reports and guidelines for fostering a culture of security.

Since 2002, **Japan's** National Incident Response Team (NIRT) has been holding seminars for public officials in charge of managing emergency communications. In 2004, the IT Security Office organised similar seminars. Moreover, all government departments are also holding internal awareness seminars for their employees.

In **Korea**, the government has established a system for sharing information security experiences and best practices. This exchange is particularly useful in case of a virus outbreak, where proactive measures are immediately taken. The IT official training centre also conducts online education activities aimed at raising government officials' information security awareness.

In the **Netherlands,** the ICT organisation of the public sector (ICTU) is tasked with the promotion of ICT within the public administration, and has carried out several information security awareness initiatives. Its Knowledge Centre Electronic Government provides an overview of all programmes and projects in the field of e-government, including information security. Moreover, several electronic authentication initiatives currently under development are also expected to foster a culture of security within government institutions in the areas of taxes, education or health care.

In **Spain**, considerable efforts have been made for fostering e-government projects and activities. In this context, particular attention is paid to information security. The national tax authorities use electronic signatures to foster online submission of tax declarations. The current integration of electronic signatures with the national identification card is also expected to further develop a culture of security among government officials.

286. www.mediakomm-transfer.de

In **Sweden**, the Commission on Information Security will deliver its final report in September 2005 which will evaluate the current programmes and initiatives, and propose a new national strategy. The Swedish Agency for Public Management has together with some other agencies procured solutions for identification and electronic signatures to be used for e-government services. The Swedish Agency for Public Management has also developed guidelines for different information security matters, *i.e.* Guidance for agencies' handling of spam. In preparing for the Year 2000 problem a legal instrument was set up to make agencies address the issues at hand, supported by oversight by the Agency for Public Management that regularly reported progress to the Government. The Swedish Agency for Emergency Management is responsible for a set of recommendations on IT-security measures for information systems critical to society (BITS). The recommendation addresses areas like organisation, policy, information and education, access management, operation and maintenance, communication, and continuity planning.[287] The Swedish Agency for Public Management is responsible for a framework of requirements and guidelines based on SS-ISO/IEC 17799 for public agencies' internal information security work (OffLIS). The guidelines and a framework are meant to support the information security in agencies. It is basically a model for classification of assets and a database of requirements matched this classification. This database contains requirements and can be developed to suit the organisation using the OffLIS framework.[288]

In the **United States**, the Federal Information Security Management Act of 2002 (FISMA) and the Office of Management and Budget (OMB) security policies are assisting federal departments to redress their information security shortcomings and weaknesses. One of the first steps in bringing some order and discipline in the information security of the federal government has been the NIST's Federal Information Processing Standard (FIPS) 99, entitled *Standards for Security Categorisation of Federal Information and Information Systems*. The standard predicates that federal departments have to determine appropriate priorities for their information systems and apply the necessary measures to protect them. In the long term, the application of this standard is expected to develop a more cost–effective, mission–oriented approach to information security management. Nevertheless, in addition to FISMA requirements, there are also standards for authentication, communication and collaboration that play a pivotal role in fostering the overall information security status of government departments.

The **Czech Republic, Norway, Portugal** and the **Slovak Republic** have not reported activities in this area.

IV. Government as partner with business and industry[289]

Question 7: Most successful government collaborative initiatives with, and outreach to, small and medium-sized enterprises (SMEs) to promote a culture of security. Initiatives currently being developed or plans for doing this in the future.

The **Australian** Government has published a booklet - *Internet Security Essentials for Small Business* — to support small business owners and operators' efforts to understand security issues. The booklet is based on a 2002 product updated with security developments relating to spam, viruses, Trojans and e-mail-based Internet fraud. Printed material is associated with online training resources.[290]

287. www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/KBMs%20publikationsserier/Rekommenderar/bits_rekomm2003-2.pdf

288. www.statskontoret.se/upload/Publikationer/2003/200323.pdf

289. This section was meant to address both the policy-oriented principles (1-5) and the operation-oriented principles (6-9) of the 2002 *OECD Security Guidelines.*

290. www.dcita.gov.au/ie/e-security/Internet_security_essentials_for_small_business

The **Austrian** federal government facilitated the integration of electronic signatures into services and applications offered by SMEs through the development of the Modules for Online Applications. The Handbook of IT-security contains specific elements for SMEs. In addition, seminars targeted at SMEs have been organised both by the "Initiative Information Security Austria" (IISA) [291] and by various universities, in particular at the "Austrian IT-Security Day 2004".[292] Further initiatives are planned for 2005, including by the Austrian Chamber of Commerce.

Canada reported three examples of initiatives: *i)* Industry Canada brought together public and private sector representatives in the Canadian e-Business Initiative (CeBI) to develop strategies for advancing the adoption of Internet-based solutions in business with a focus on SMEs. The CeBI project identified the need for raising security and privacy awareness with SMEs and developed Web sites, information packages, seminars and assessment tools for the SME community. *ii)* The "E-Biz.enable" [293] program of the federal government led to the development of a Web site aiming at educating businesses and SMEs about safety measures, tools and techniques to ensure a secure environment. *iii)* PrivacyForBusiness[294] is a government Web site for businesses which serves as a one-stop-shop helping to become compliant with Canada's private sector privacy legislation (the Personal Information Protection and Electronic Documents Act – PIPEDA).

Denmark continuously dialogues with business representatives and gathers statistical information on IT security in business and industry.

In **Finland**, the Confederation of Finnish Industries[295] (EK), which represents the entire private sector, has implemented many actions in relation to SMEs. The Finnish Information Society Development Centre[296] (TIEKE), a neutral and non-profit organisation, has a networking role in promoting efforts of its members within the public and private sectors to create viable tools and expertise for use in the information society.

France has set up a unit (AsTEC) for technical assistance to the industry, including innovative SMEs, in the design and specification of security products for which official certification is sought. Short-term assistance is provided for clearly identified projects. AsTEC participates in national and international conferences and plays a role in the definition of the government's needs for security products, and in the orientation of research and development in this area.

Germany reported three initiatives:

- The "Secure Use of Internet for Medium Sized Enterprises" Web site ,[297] launched in early 2004 by business associations and companies with technical support from the Federal Office for Information Security, consists of easy-to-understand material and practical examples from companies to help SMEs protect themselves against security threats (viruses, hacker attacks, etc.). Some topics are organised by industry domain, company size and number of computers.

291. www.iisa.at/iisa/

292. www.syssec.at/Sicherheitstag/

293. http://strategis.ic.gc.ca/epic/Internet/inee-ef.nsf/en/h_ee00207e.html

294. www.privacyforbusiness.ic.gc.ca

295. www.ek.fi

296. www.tieke.fi

297. www.mittelstand-sicher-im-Internet.de

Industry-specific material has been developed in an active dialogue with associations from selected industries.

- Mcert is a fee-based neutral and manufacturer-independent competence centre for IT security. It provides SMEs with specifically tailored, understandable and reliable security information and recommendations for action, including warnings of malicious programs and information concerning security gaps. The information is sent by e-mail and archived in a searchable database. Mcert is a public-private partnership led by the German Association for Information Technology, Telecommunications and New Media e.V. (BITKOM[298]) together with the Federal Ministry of the Interior, the Federal Ministry of Economics and Labour, and partners from industry.

- The IT Baseline Protection initiative of the Federal Office for Information Security is composed of three elements:

  – The IT Baseline Protection Manual contains standard security measures for typical IT applications and systems with normal protection needs. The associated baseline protection tool (GS Tool) supports the development of a security concept.

  – A certification framework[299] was launched in 2003. More than 100 auditors have been licensed for auditing the technical and organisational implementation of IT baseline protection. 10 certificates were issued by the end of 2004.

  – The IT Security Guidelines[300] provide a concise and understandable overview of the most important security measures, focusing on organisational measures and practical examples.

In addition, sample guidelines and examples of concepts were published in 2004.[301] A publication "Examples of profiles for small institutions and SMEs" is planned.

Japan combines organisational, financial, informational/educational measures. The government has created a Committee of Information Security Governance which started its work in September 2004, including security benchmarks. Financial support is provided through government's loans and investment programmes for IT users and suppliers, and tax support for companies buying network security and maintenance equipment. Furthermore, two Web sites have been created: the counter-cybercrime Web site[302] (2001) releases information about the current situation of cybercrime, countermeasures and police contact points; and the "MIC Information Security Site for the People" (March 2003) informs the people about government measures for information security. Finally, the Information-technology Promotion Agency (IPA) and JPCERT/CC[303] hold seminars on countermeasures against computer virus and unauthorised access.

298. www.bitkom.org

299. www.bsi.bund.de/gshb/index.htm (German/English).

300 www.bsi.de/english/gshb/guidelines/index.htm (English).

301. www.bsi.de/gshb/deutsch/musterrichtlinien/index.htm (German) - www.bsi.de/gshb/deutsch/hilfmi/beispielprofile.htm (German).

302. www.npa.go.jp/cyber

303. The Japan Computer Emergency Response Team Coordination Center.

The **Korean** Ministry of Information and Communication (MIC) conducts online and on-site check-ups for SMEs which have low-level security. In addition, MIC offers training for system managers and organises CEO gatherings to encourage the security investments and raise security awareness. The initiative 'Online Information Security Training Lab' also offers training programmes and will target SMEs in 2005.

In the **Netherlands**, the Alerting service[304] (*Waarschuwingsdienst*) for citizens and SMEs is provided by GOVCERT.NL in co-operation with the Ministry of Economic Affairs. Through a Web site, a free mailing list and a free SMS service, the service provides users with up-to-date information on security incidents (early warnings and alerts), and background information on ICT security issues. A location-based SMS service is under discussion with telecom providers. Created in February 2003, the service has 33 146 members on the mailing list, and 35 227 visits/day on the Web site.

The "Surf op Safe"[305] national awareness campaign on the safe use of the Internet targets consumers and SMEs.

In **Spain**, a campaign of 21 workshops targeted at SMEs[306] has been organised, dealing with security and trust on the Net. The workshops included the presentation of security applications using electronic signatures. Other initiatives of special value for micro-enterprises have been organised, for example meetings carried out in co-operation with the Internet Users Association. Additional initiatives have been taken by the Red.es Antivirus Early Alert and Computing Security Center (Red.es CATA).

In **Sweden**, the National Post and Telecom Agency has published information on Internet security directed at citizens and SMEs, based on their own expertise and public consultation.[307] Many ISPs and agencies offering Internet connections and Internet-based services to citizens and businesses provide links to this Web site. An automatic test has been made available for those who would like to check their security level. In 2005 a private sector led initiative was launched in co-operation with leading agencies, aimed at consumer's security concerns and behaviour. The campaign was launched with an event in Stockholm with speakers from the involved companies, agencies and the minister responsible for the issues.[308] The event is to be followed by regional and local events throughout Sweden.

In the **United Kingdom**, a suite of materials aimed at smaller companies has been developed, including a self-assessment tool,[309] and supported by surveying to understand how companies are responding to the changing nature of information risk.[310] The National High Tech Crime Unit (NHCTU) has recently issued a guide for small and medium-sized enterprises on information security, providing basic information on protecting computers and the data stored within a network.

In the **United States**, the National Cyber Alert System (NCAS) provides home users and small businesses with information about imminent threats and incidents, periodic "cyber-tips", best practices and "how-to" guidance messages written in a technical and non-technical format. DHS co-sponsors the

304 www.waarschuwingsdienst.nl

305. www.surfopsafe.nl

306. www.setsi.min.es/progarte/arte.htm

307. www.pts.se/Internetsakerhet

308. The original inspiration for the campaign was the Finnish national information security day. Cf. the campaign Web site at www.surfalugnt.se/

309. www.dti-bestpractice-tools.org/healthcheck

310. www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf

National Cyber Security Alliance (NCSA) and StaySafeOnline, a public-private organisation created to educate home users, small businesses, K-12 and higher education audiences on cyber security best practices. The NCSD/US-CERT also sponsors Common Vulnerabilities and Exposures (CVE) for SMEs and larger businesses for mitigating common vulnerabilities across enterprise-wide networks. The FTC has established a public awareness programme which includes information on how users can protect their computers from hackers and other computer threats.[311] The Small Business Administration (SBA) also has an online training program targeting SMEs called "Be Aware and Prepare".[312] Several organisations (NIST, SBA, FBI, Chamber of Commerce, NCSA) are in the process of assessing the effectiveness of the various approaches and materials.

Portugal plans to specifically target SMEs in its IT security communications strategy, as part of a strategy to create national awareness of information security in its project for a National Information Security Framework.

The **Czech Republic** and the **Slovak Republic** have at present no initiatives in this field, nor are such activities planned for the future. **Norway** reported no initiatives for this question.

Question 8: Most successful initiatives and approaches used by government for outreach to business and industry to foster a culture of security among business and industry and develop public-private co-operation in nine areas, including initiatives and approaches planned for the future.

a) Awareness-raising

In addition to the initiatives outlined under question 7 (awareness campaigns specifically aimed at SMEs), respondents reported the following:

Australia, in recognition that around 90% of the critical infrastructure in the country is owned and/or operated privately, has created a "Trusted Information Sharing Network" in which the Government works directly with owners and operators of critical infrastructure to help protect it from all hazards, both human and naturally instigated.[313] Australia also has a national technical Computer Emergency Response Team (AusCERT), a non-government, not-for-profit organisation.[314] The Australian Government contracts services from AusCERT such as the free National Information Technology Security Reporting and Alert Scheme.[315]

The *Computer Incident Co-ordination* **Austria** (CIRCA)[316] is a public private partnership designed as an information and action network at the national level, with multidisciplinary incident experts from ISPs,

311 www.ftc.gov/infosecurity

312. www.sba.gov/training

313. Cf. question 2c) above.

314. Cf. www.auscert.org.au

315. This scheme, launched in May 2003, allows computer users to receive alerts about common computer threats and vulnerabilities, and provides a method of reporting suspected security incidents. AusCERTs wide range of information sources, including other CERTs, software and antivirus vendors and IT research organisations from around the world, enable it to provide accurate, up-to-date and relevant alerts and warnings. AusCERT analyses data it collects from the scheme to determine whether there is an emerging threat or pattern of attacks to assist with prevention, detection and response to security incidents.

316. Cf. www.circa.at

IT-security firms, operators of critical infrastructures, companies with big networks and organisations from the public sector.[317]

The Government of **Canada** has co-operated with the Canadian e-Business Initiative (CeBI), a private sector-led partnership and its predecessor, the E-Business Opportunities Roundtable, on the issue. CeBI's Online Privacy & Security Team particularly aimed at providing practical tools to assist SMEs in overcoming online privacy and security related concerns. Various information and assessment tools were made available online and a mail-out insert that directs recipients to the PrivacyForBusiness.gc.ca Web site was sent to over a million business recipients in June 2003 through Canada's Custom and Revenue Agency's monthly Goods and Services Tax mailing.

Denmark will launch a cross-sector national IT-security awareness campaign in March 2005. The Danish Government is managing this project, with other stakeholders providing funding, knowledge and specific activities.

In **Finland**, the National Information Security Day is an annual event held in February. It is organised jointly by various public-sector bodies, private-sector businesses and other organisations. The purpose is to increase awareness of current threats to information security and practical measures for protection against these threats.[318] The Government Information Security Management Board (VAHTI) has prepared questionnaires and multimedia material for co-ordinating the awareness programme, available in every agency.

The **German** Federal Office for Information Security (BSI) regularly participates with a trade show booth in the main IT fairs in Germany.[319] In addition, the Office hosts conferences and other events dedicated to information security.[320]

Japan, has launched the "MIC Information Security Site for the People" in March 2003 to provide means and knowledge regarding information security to citizens. In addition, the Information Technology Promotion Agency (IPA) and JPCERT/CC[321] hold nationwide seminars on countermeasures against computer viruses and unauthorised access for managers of information systems. Furthermore, the NPA counter-cybercrime Web site[322] and the NPA security portal site '@police' provide content for enterprise network administrators, such as countermeasures against unauthorised computer access, 'Security Online Lectures', 'Cases Suffered from Cybercrime and How to Deal With It' and 'Vulnerability Information'.

317. Cf. question 2b) above.

318. Cf. www.tietoturvaopas.fi/ (general information) and www.tietoturvakoulu.fi (Information Security Day 2005). Cf. also question 2g) above.

319. These are: CeBIT (Hannover), Systems (Munich), and Security (Essen).

320. Recent events include the "IT-Grundschutz-Tag" (IT baseline protection conference, Köln/Cologne, April 2004); a presentation at the "Moderner Staat" (modern government) trade show, the 5th International Common Criteria Conference (ICCC, Berlin, September 2004); the regular organisation of common criteria workshops, a conference series offered by the Federal Office for Information Security for board members, executive managers and politicians, and the organisation of the "9. Deutscher IT-Sicherheitskongress" (9th German IT security congress, May 2005, Bonn). This bi-annual congress presents up-to-date IT security trends and issues, and attracts around 500 visitors from business, public administration and research.

321. The Japan Computer Emergency Response Team Coordination Center

322. www.npa.go.jp/cyber/

To draw attention to and encourage investments in information security, the **Korean** Ministry of Information and Communication (MIC) awards an 'Information Security Grand Prize' to enterprises and organisations that put information security into good practice.

In the **Netherlands**, the most successful initiatives in co-operation with business partners and industry are the *Kwetsbaarheid op Internet* (KWINT) programme, ECP.nl,[323] GOVCERT.nl, Nacotel[324] and the project "Protection of the Critical (Information) Infrastructure".[325] All of these initiatives are examples of public-private partnerships (PPP).

KWINT,[326] founded in 2002, is a platform where government, non-governmental and private organisations discuss issues in the domain of Internet security. More than 70 partners are involved including several ministries, the national police agency (KLPD), universities, research institutes, branch organisations, banks, and the Amsterdam Internet Exchange (AMS-IX). A relevant part of the programme is to raise the awareness of companies, especially SMEs. Other target groups are consumers, large companies, and the public sector. In the future the government will probably extend the scope of KWINT to other ICT areas (*e.g.* vulnerability of the infrastructure). The KWINT programme will end after 2005; continuation of the programme depends on a review of the government's e-security policy.

ECP.nl is the platform for eNederland (www.ecp.nl). One of seven main objectives for 2005 is work on security and reliability of ICT systems and networks. The platform disseminates knowledge and experience to its target groups and organises meetings and working groups on subjects like customer trust, explanation of legislation and regulations, security of ICT applications, open standards and new (international) developments in IT. Working groups monitor the developments on a permanent basis and translate these into concrete activities (services, seminars, publications, lobbying).

Portugal plans to address awareness raising in the framework of its project for a National Information Security Framework, as part of a strategy to create national awareness on information security.

In **Spain**, one of the most successful awareness events was the *Information Security Certification Meeting* with more than 210 participants. Organised by the Directorate-General for Information Society Development, this meeting targeted corporate general and IT systems management, and addressed implications of a security-focused management, pointing out international best practices to be followed. Another focus was on certification procedures, including practical application examples from enterprises. In addition, Spain has realised a project for *Information Systems Security Fora* (FOROSEC), financed in the PROFIT program of the Spanish Industry, Tourism and Commerce Ministry. FOROSEC is a thematic network on security, composed of five technology centres specialising in information and communications technologies, to provide organisations with a network focused on *i*) new technologies in security; *ii*) enhancing electronic business services, and *iii*) improving technological capacity and competitiveness.[327]

---

323. ECP.nl (Platform for e-Netherlands) is responsible for the organisation and facilitation of the KWINT platform and the working groups. The subjects of the current working groups are risk-analysis, communication, safe Internet for children, security policy and security measures in an organisation, continuity of the Internet, expert group cybercrime, education and transparency by quality information. The results of these working groups are guidelines, quick-scans, reports, and policy development.

324. Cf. question 2c) above.

325. Cf. question 2c) above.

326. www.kwint.org

327. Cf. www.forosec.com.

In the **United Kingdom**, the Government has developed strong public/private partnerships, and also participates in many private sector initiatives.[328] In particular, the project "Endurance" is running a public relations campaign aimed at home users and micro businesses to make them aware of the need for basic computer hygiene and responsible behaviour on the Internet, which involves several government departments and private sector partners.

In the **United States**, the *National Cyber Alert System*, launched by the US-CERT in January 2004,[329] provides detailed and accurate information about imminent threats and incidents through alerts and general cyber security information in a periodic series of "cyber tips," "best practices," and "how-to" guidance messages. To help educate home users and small businesses, regardless of computer skill-levels, the alert system provides information in both technical and non-technical formats.[330] In parallel, the National Cyber Security Division (NCSD) and US-CERT are increasing their outreach to industry and associations, as well as investigating other vehicles to distribute information to as many Americans as possible through the alert system.

The Department of Homeland Security (DHS) closely co-ordinates cyber awareness activities with other government agencies such as the Federal Trade Commission (FTC). The FTC has established a public awareness programme that provides resources about computer and Internet use to individual consumers.[331]

In addition to these efforts, the *Information Sharing and Analysis Centers* (ISACs), and the emerging *Sector Co-ordinating Councils (SCCs)* provide another mechanism for public-private information sharing on cyber security issues.[332]

NCSD has also established a relationship with the *"Multi-State Information Sharing and Analysis Center" (MS-ISAC)* for information sharing and outreach to state and local governments in the US regarding cyber security issues. One specific joint NCSD and MS-ISAC initiative is a series of national Web casts on cyber security issues.[333]

To promote awareness among the general public, DHS co-sponsors the *National Cyber Security Alliance* (NCSA). NCSA is a coalition of companies, trade associations, organisations and government bodies that have joined forces to educate Americans about computer security, and encourage all computer users to protect their home and small business systems. NCSD has provided funding to expand and support a variety of initiatives, including consolidation and development of the "Top Ten Cyber Security

328. See the "SAINT" report referenced in the UK answer to question 2e) above.

329. On day one of the launch, the US-CERT Web site had more than one million hits. Today, more than 270,000 direct subscribers receive National Cyber Alerts to enhance their ability to prepare for, mitigate, and respond to cyber events.

330. Since the release of the system, the Department of Homeland Security (DHS) has issued a variety of material on topics such as: "Understanding Firewalls"; "Good Security Habits"; "Choosing and Protecting Passwords"; and "Why is Cyber Security a Problem?"

331. Including security awareness information about how consumers can protect their computers from hackers and a variety of widespread viruses and other attacks.

332. ISACs and SCCs have been created in the identified critical infrastructure sectors to coordinate industry and industry-government sector data sharing and analysis regarding vulnerabilities and incidents. As industry sector groups foster increased awareness and efforts in critical infrastructure protection, ISACs and SCCs have become a crucial part of the public-private partnership toward greater cyber security.

333. Available on the US-CERT.gov Web site.

Tips"[334] Web site with cyber security best practices for home users (including children) and small businesses, and for the launch of Cyber Security Awareness month.[335]

In December 2003, DHS co-sponsored a *National Cyber Security Summit* to galvanise private sector efforts toward greater cyber security. In conjunction with the Summit, private industry and association participants formed the *National Cyber Security Partnership*.[336] One of its five *task forces*[337] comprised of cyber security experts from industry, academia and government, has issued a report on *Awareness for Home Users and Small Businesses.*[338]

After the release of the reports and recommendations of its task forces in spring 2004, the organisation continues to meet and collaborate on implementing the recommendations and continuing the public-private partnership on cyber security.

b) Education and training, including distance learning

Many respondents reported co-operative initiatives with business and industry with regard to education and training, including:

Finland reports training activities to be part of the yearly planning in the public sector. In addition, electronic material and publications which support training are available from the Finnish Government Information Security Management Board (VAHTI).

In **France**, the Central Directorate for Information Systems Security (DCSSI) is currently working to put training modules on line, to make training available as widely as possible, and especially to businesses. An initial module on digital signatures is already available on the Web site,[339] and a second one, on risk assessment, is forthcoming.

---

334. Available for free at www.staysafeonline.info/

335. Additional activities in partnership with NCSA include the following: *i*) In partnership with the Fairfax Chamber of Commerce and NIST, NCSD hosted an educational training seminar on cyber security for small business which outlined key issues for improving organisations' cyber security posture; *ii*) In partnership with AOL, NCSA conducted and analyzed the largest national in home study of home computer users online threats, perception and gaps; *iii*) Sponsored the "Staying Safe in the Cyber World" event to teach elementary and high school students about safe online practices *iv*) Conducted a NBC live home computer assessment titled "Is your computer virus free?"; and *v*) Conducted an industry-wide perception poll to identify current cyber security perceptions and trends.

336. The National Cyber Security Partnership (NCSP) is led by the Business Software Alliance (BSA), the Information Technology Association of America (ITAA), TechNet and the US Chamber of Commerce in voluntary partnership with academicians, CEOs, federal government agencies and industry experts. Cf. www.cyberpartnership.org.

337. Cf. www.cyberpartnership.org/init.html

338. This task force works to follow up on the outreach initiated by the National Cyber Security Alliance, through such online programs as Stay Safe Online, and Cyber Citizen. It focused on best practices in education and awareness, and made suggestions for how a public/private national outreach awareness campaign could reach 50 million home users and small businesses within one year, using paid and earned media, ISP's, security vendors, and other outlets. Cf. www.cyberpartnership.org/init-aware.html. Other task forces addressed: Cyber Security Early Warning; Corporate Governance; Security Across the Software Development Life Cycle; and Technical Standards and Common Criteria

339. www.formation.ssi.gouv.fr

Germany, through the Federal Office for Information Security, makes information available on security to users from public administrations, as well as to IT manufacturers and suppliers from industry.

Japan opened in March 2003 the "MIC Information Security Site for the People", to provide means and knowledge regarding information security to a broad audience. In addition, each Prefectural Police visits companies in critical information infrastructure sectors individually, and provides them with security information gathered by NPA. Furthermore, each Prefectural Police holds seminars on information security, in co-operation with critical information infrastructure industry sectors, and training exercises in response to cyberterrorism.

Since 2001, the **Korean** Ministry of Information and Communication (MIC) has been operating the 'Online Information Security Training Lab', where information security managers are offered various technology training programs to enhance their abilities to prevent and respond to security incidents. The Ministry also offers various educational programmes for information security experts.

Spain has realised a project for Information Systems Security Fora (FOROSEC).[340]

In the **United Kingdom**, the Government is working with academia and the private sector to establish a new professional body to increase the professionalism and standing of information security professionals.

In the **United States**, the US Government has undertaken several initiatives in partnership with research and academic communities to better educate and train future cyber security practitioners. In March 2004, the Department of Homeland Security (DHS) signed a Memorandum of Agreement (MOA) with the National Security Agency (NSA) to co-sponsor the *National Centers of Academic Excellence in Information Assurance Education* (CAEIAE) programme and to expand it into a national programme.[341] DHS also signed an MOA with the National Science Foundation (NSF) in March 2004 to cosponsor and enhance the Scholarship for Service (SFS – "*Cyber Corps"*) program, funding the final two years of students' bachelors, masters, or doctoral study in information assurance.[342] In addition to the SFS Program, the NSF created the *Cyber Trust program* to co-ordinate and expand its research efforts in the areas covered under the Cyber Security Research and Development Act (CSRDA), and train graduate students in research and development, for significantly increase the nation's cadre of professional researchers and cyber security educators. Furthermore, a joint *DHS/Treasury Computer Investigative Specialist (CIS)* program trains federal criminal investigators in basic computer forensics. To establish greater consistency and reliability among skill certifications, the Department of Homeland Security (DHS) and the Department of Defence (DOD) have partnered to create a national-level job task analysis (JTA).[343] A task force of the

340. Cf. www.forosec.com, and question 8a) above.

341. Currently, there are 59 universities in 26 states and the District of Columbia designated as National Centers of Academic Excellence.

342. Cf. question 10 below.

343. According to the US National Cyber Security Strategy, "Certification [of qualified persons] can provide employers and consumers with greater information about the capabilities of potential employees or security consultants." Although more than 90 cyber security-related certifications currently exist, no comprehensive job or skill standard has guided certification development. The JTA will identify the knowledge, skills, and abilities associated with information assurance jobs to provide a clear baseline against which industry certifications can be developed. Currently underway, the end product will be a national-level JTA that (1) describes skill standards for information assurance for both the public and private sector; (2) provides a baseline that will allow industry certifications to be mapped to specific jobs; and (3) clarifies the job skills upon which to build future certifications.

National Cyber security Partnership (NCSP) issued in spring 2004 a report on cyber security early warning.[344]

c) Watch and warning and emergency response

Most respondents have CERTs or CERT-like institutions in place, some of which are operated by public private partnerships (cf. section 2b), and usually target specific audiences. In addition, the following initiatives have been reported specifically with regard to collaborative efforts between governments and the private sector on watch and warning, and emergency response:

The **Australian** Government, in recognition that around 90% of the critical infrastructure in the country is owned and/or operated privately, has created a "Trusted Information Sharing Network" (TISN), in which the Government works directly with owners and operators of critical infrastructure to help protect it from all hazards, both human and naturally instigated.[345] Australia also has a national technical Computer Emergency Response Team (AusCERT), a non-government, not-for-profit organisation. The Australian Government contracts services from AusCERT, such as the free National Information Technology Security Reporting and Alert Scheme.[346]

The **Canadian** federal Department of Public Safety and Emergency Preparedness (PSEPC) has established the Canadian Cyber Incident Response Centre (CCIRC) as a focal point for dealing with cyber threats and incidents impacting Canada's critical infrastructure 24 hours a day, 7 days a week.[347] PSEPC has also developed a National Exercise Program designed to enhance emergency management operational readiness, including cyber protection, by promoting, facilitating and co-ordinating exercises involving federal departments, provincial, municipal, international and private sector partners, and has prepared a Guide to Business Continuity Planning.[348]

A private sector company (EWA Inc) has been operating a Canadian Computer Response Team ("CanCert") since 1998. The Canadian National Critical Infrastructure Assurance Program (NCIAP) promotes a national partnership among private and public sector stakeholders.[349]

In **Japan**, ISPs and vendors have co-operated in establishing the "Telecom-ISAC Japan", a private organisation that collects, analyses and shares security information among members and with other co-operating foreign organisations. Furthermore, the Ministry of Economy, Trade and Industry (METI), the Information Technology Promotion Agency (IPA) and JPCERT/CC[350] operate a Traffic Monitoring system

344. This task force tracked a national cyber security response system, to improve the sharing, integrating and disseminating of information about vulnerabilities, threats and incidents among distributed information systems, at both the technological level and the organisational, human level. The goal is to build a system in which critical information is distributed in a timely way before an incident occurs. Cf. www.cyberpartnership.org/init-early.html

345. Cf. question 2c) above.

346. Cf. http://national.auscert.org.au, and question 8a) above.

347. Cf. question 2b) above.

348. available under "Information Products" at www.ocipep.gc.ca/info_pro/self_help_ad/general/busi_cont_e.asp. The Guide stresses the need for continuity plans for critical services or products to be continually delivered to clients. PSEPC advocates a business continuity plan that endeavours to ensure that critical operations continue to be available, instead of focusing on resuming business after critical operations have ceased, or recovering after a disaster.

349. Cf. question 2c) above.

350. the Japan Computer Emergency Response Team Coordination Center

on the Internet, as well as a "Vulnerability Handling Framework". The NPA security portal site '@police' is used to provide information to the public in case of emergency. The NPA also issues warnings and provides information to the public on viruses/worms, and other malicious activities on the Internet, including analysis of data collected from intrusion detection systems (IDS) and firewalls installed nationwide at police institutions.

In **Korea**, the Ministry of Information and Communications (MIC) has established the Korea Internet Security Center (KISC) in the Korea Information Security Agency (KISA) and operates an urgent incident response system for early detection and analysis of Internet security incidents, and issuance of warning signals, in co-operation with information/telecommunication service providers.

Spain, besides operating the Antivirus Alert Center in the framework of Red.es, has realised a project for Information Systems Security Fora (FOROSEC).[351]

The **Swedish** IT Incident Centre, although fully funded by the government, works closely with representatives from private companies, both operationally and on strategic issues. The Swedish Emergency Management Agency (SEMA) has initiated an information exchange programme (according to a British concept) in order to promote public-private partnerships. The purpose of the programme is to develop a trustful information exchange about threats and vulnerabilities between actors within specific areas.

In the **United Kingdom**, the Government has as part of its efforts regarding Critical National Infrastructure (CNI) looked at new ways of distributing real time alert and warnings through communities of interest using standard terminology and software. This is part of the WARP (Warning Advice and Reporting Points) concept. There is also a simpler alert service via e-mail or SMS for any user – ITsafe.[352]

In the **United States**, the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS) has created the US Computer Emergency Readiness Team (US-CERT) – a partnership between NCSD and the public and private sectors. US-CERT is the operational arm of NCSD's cyber analysis and incident response activity.[353]

d) Corporate Governance and ethics

The Conference Board of **Canada,**[354] working in collaboration with other conference boards around the globe, has developed a series of assessment tools, best practices, and various other materials to promote good corporate governance and business ethics.

In **Japan**, the need for action with regard to information security is explained to corporations and executives on the "MIC Information Security Site for the People". Furthermore, the Ministry of Economy, Trade and Industry (METI) promotes an Information Security Management System (ISMS) certification scheme in the private sector. To promote information security governance within corporate management, METI has also set up the *Committee of Information Security Governance* in September 2004.[355]

---

351. Cf. www.forosec.com. For a more detailed description of the initiative cf. question 8a) above.

352. Cf. question 2b) above.

353. Cf. footnote 93.

354. Cf. www.conferenceboard.ca

355. This committee will *inter alia* discuss the issue of IT security benchmarks.

The **Korea** Information Security Agency (KISA) grants 'Information Security Management System Certification' to information/telecommunication service providers who establish and operate proper information security management systems to secure their communication networks.

In the **United Kingdom**, the Government has started to shift the discussion away from point solutions to security into a broader concept of information risk management within a corporate governance framework. Instrumental in this has been the dialogue between the private and public sectors and, in particular, the creation of the ISO 17799 and the BS 7799 Part 2 standards.

The **United States** reported that concern for governance and ethics is reflected throughout the US approach to security of information systems and networks. In the framework of the "National Cyber Security Partnership",[356] a CEO-led task force specifically set up for dealing with the matter published a report in spring 2004, which identified *cyber security roles and responsibilities within the corporate management structure*, referencing and combining best practices and metrics that bring accountability to key elements of a cyber security system.[357]

e) Creation and implementation of corporate security policies

Austria has developed an *IT Security Handbook*, intended to help those responsible for IT to draw up a reliable IT security policy for their organisation, and to contribute to the creation of a standard approach in the field of IT security.[358]

Industry **Canada** and the Canadian e-Business Initiative (CeBI)[359] have developed a Web site, specifically to help SMEs understand security and privacy risks associated with conducting business online,[360] and help them to conduct risk assessments and develop security policies.

In **Germany**, the Federal Office for Information Security has developed the "IT Baseline Protection Manual", and a tool for facilitating the implementation of its recommendations, together with reference material for the development of information security policies and guidelines, and a process for voluntary certification. In addition, the Office hosted an "IT baseline protection conference" (*IT-Grundschutz-Tag* – Köln/Cologne) in April 2004.

In **Japan**, the Ministry of Economy, Trade and Industry (METI) promotes the introduction of an Information Security Management System (ISMS) certification scheme in the private sector. Each Prefectural Police is working with companies in critical information infrastructure sectors to create and improve information security policies.[361]

---

356. Cf. question 8a) above.

357. The report is available at www.cyberpartnership.org/init-governance.html

358. *Österreichisches IT-Sicherheitshandbuch*, Chief Information Office, ICT-Staff Unit, *Teil 1: IT-Sicherheitsmanagement* Version 2.2 November 2004 and *Teil 2: IT-Sicherheitsmaßnahmen* Version 2.2 November 2004, www.cio.gv.at/securenetworks/sihb/

359. Cf. question 7 above.

360. http://privacyguide.cebi.ca

361. *E.g.* through individual visits. In addition, the Prefectural Police also works with those companies which have already established information security policies, to implement education programmes and to revise them corresponding to the social changes.

In **Korea**, through the private sector information security diagnosis system, the Korea Information Security Agency (KISA) has defined criteria for security diagnosis and has established a portal site[362] to let enterprises test their information security environments by themselves.

Portugal plans to address the issue in its project for a National Information Security Framework, assisting entities in developing their own information security policies, based on the ISO/IEC 17799 standard.

In the **United States**, the government's efforts relate to and support the creation and implementation of corporate security policies; however, each corporation is responsible for developing its own policies.

f) Prevention and combating cybercrime

In **Australia** the Australian High Tech Crime Centre (AHTCC) formed the *Joint Banking & Finance Sector Investigations Team* (JBFSIT) in May 2004 in recognition of the need for industry and law enforcement agencies to work closely together, particularly in relation to critical infrastructure sectors. The JBFSIT, comprised of police investigators, seconded staff from the banking institutions and intelligence analysts, was created to investigate instances of online banking fraud, including phishing.

Although **Canada** has strong laws that apply to cyberspace, the Government of Canada recognises that legislation alone will not solve the problems of illegal and offensive content on the Internet. The federal government's approach is to involve a broad spectrum of Canadians in addressing the issues.[363] In 1996, the *Canadian Association of Internet Providers (CAIP) developed a voluntary code of conduct* for its membership. Under this code, CAIP members agree to *i*) co-operate with all government officials, international organisations and law enforcement authorities seeking to clarify the responsibilities for each of the different functions performed by Internet companies, *ii*) to comply with all applicable laws, and *iii*) to not knowingly host illegal content, and to share information about illegal content for this purpose. Industry Canada is working with CAIP to strengthen the effectiveness of the code by supporting CAIP's Fair Practices Initiative.[364]

The *Information Technology Association of Canada (ITAC) - Cyber Security Forum* brings together the private sector, government, and law enforcement agencies, to develop joint solutions in three areas: cybercrime, cryptography policy and critical infrastructure protection. In addition to holding regular meetings, the Forum sponsors a variety of events and information sessions on security challenges and potential responses to them.

In **Finland**, addressing computer crime as an information society problem is one of the priority projects recommended for 2005 by the National Information Security Advisory Board.

---

362. www.boho.or.kr

363. Its priorities include: *i*) supporting initiatives that educate and empower users; *ii*) promoting effective industry self-regulation; *iii*) strengthening the enforcement of laws in cyberspace; *iv*) implementing hotlines and complaint-reporting systems; and *v*) fostering consultation between the public and private sectors, and their counterparts in other countries. The government closely monitors developments at home and abroad, and encourages and sponsors research and analysis to build a broader understanding of the scope of the issues and the range of available solutions. Cf. www.cyberwise.gc.ca/english/chap2_e.html

364. The Fair Practices Initiative will expand the scope of the code, and will provide guidance to CAIP members about how to put self-regulatory measures into practice on a day-to-day basis. CAIP is also exploring the feasibility of making the new fair practices enforceable rather than voluntary, with an economical and efficient means of dispute resolution.

Japan is setting up tax support measures for companies and private operators buying network security enhancement and maintenance equipment. In addition, there is financial support based on the government's loan and investment programmes for IT users and suppliers to promote procurement and production of secure systems and products. The Ministry of Economy, Trade and Industry (METI) has, in collaboration with non-profit organisations, held nationwide seminars on countermeasures against computer viruses and unauthorised access for general IT users. In parallel, the Information Technology Promotion Agency (IPA) and JPCERT/CC[365] hold similar nationwide seminars for managers of information systems. The National Police Agency (NPA) has published the results of research about unauthorised computer access and its countermeasures, on technical trends in access control and other related issues, on the NPA counter-cybercrime Web site.[366] The NPA security portal site '@police' provides security-related content for enterprise network administrators. The NPA also gives warnings and provides information on viruses/worms and other malicious activities on the Internet to the public through its Web site, including reports on the analysis of data collected from intrusion detection systems (IDS) and firewalls installed nationwide in police institutions.

Korea has been reinforcing the ability to respond to cybercrimes through the Consortium of CERTs (CONCERT) established in 1996 to share information and technologies, and to foster co-operation among CERTs at the working level.

In the **United States**, the Department of Justice is a frequent speaker on computer and network security issues and cybercrime enforcement at industry events. Furthermore, Department prosecutors have addressed insurance industry groups to promote the underwriting of policies to cover cyber-risks. Prosecutors also regularly speak to representatives from numerous industries on network security, cybercrime prevention and communication with law enforcement. In addition, the Department has worked with various technology industries to establish protocols for reporting cybercrime and working with law enforcement during criminal investigations.

g) Development of secure software

In **Austria**, a number of secure software applications are provided by the government with the "Modules for Online Applications" (MOA), in particular for the creation and verification of electronic signatures, for secure identification using the Austrian citizen card, and for electronic delivery of documents. These MOA modules are procured by the government and offered for licensing to both the public and the private sector for free. In addition, a "security layer specification" was implemented and published as freely available software together with a reference implementation. Also, some reference implementations are available, for example, for electronic payment or for verification of electronic notifications. Furthermore, a "testmail service" is offered by the government.[367] The private sector also provided some security layer implementations: Currently two Austrian software products are suitable for presenting data to be signed to the signatory ("secure viewer"): "trustview" (which won a public tender) and "hot:Sign".[368] Another product ("MBS-Sign"[369]) can be used for creating electronic signatures with a

365. The Japan Computer Emergency Response Team Coordination Center.

366. Cf. www.npa.go.jp/cyber/

367. The "testmail service" allows for checking whether e-mail systems are compatible with standards and minimum response times laid down by the Austrian e-mail policy. Any deviations from the required performance of the mail client can be identified. Specifically, encrypted, signed and clear-text mails are generated and sent to a selected recipient. The service is provided free of charge by the ICT Strategy Unit. Cf. www.cio.gv.at/applications/mailtest/ or http://sl.cio.gv.at/mailtest/MailServlet

368. "hot:Sign" is a client for creating electronic signatures using a secure signature creation device. Cf. www.bdc.at/30.html

secure signature creation device, legally equivalent to handwritten signatures. The security of these products has been confirmed by A-SIT.[370]

In **Canada**, the Canadian Advanced Technology Alliance (CATA) has expanded its support and promotion of the advanced security industry in Canada and the role of technology companies in supporting security initiatives.[371] One element of this effort is the *Advanced Security Profile*, a 200-page report of the Canadian Advanced Technology security industry. It documents security solutions that use information and communications technology (ICT) to meet a growing range of security applications and customer needs.[372]

In **Germany**, the "TeleTrusT e.V."[373] and the "T7 group[374]" have developed "ISIS-MTT", a common specification for electronic signatures, encryption and public key infrastructures. For the purpose of implementing the ISIS-MTT specification, a test concept and a test specification were made available, and a test bed was developed.[375]

In **Japan**, the IPA conducts research on secure operating systems.

The Korea Information Security Agency (KISA) performs research and development for security incident response technologies through research into up-to-date hacking and virus techniques, while the Information Security Research Division at the Electronics and Telecommunications Research Institute (ETRI) focuses on future information security technologies such as RFID and Ubiquitous Sensor Networks (USN) security.

In **Sweden**, the government is a large procurer of software and there are some initiatives to increase the usage of public procurement based on the ISO/IEC 15408 and ISO/IEC 17799 standards to foster security in IT-products and services.

---

369. "MBS-Sign" is a client intended for use with the multi-bank standard, which allows customers to manage several checking accounts with the same software. Cf. www.bdc.at/28.html

370. The "Austrian Center for Secure Information Technology" (A-SIT) is a notified body according to Article 3(4) of the EU Electronic Signature Directive 1999/93/EC.

371. Cf. http://209.87.231.94/HomelandSecurity/. The objectives of CATA's "Homeland Security" initiative include: *i*) to contribute to the better security of Canada and its citizens, in a manner consistent with Canadian values and beliefs; *ii*) to address physical and information security within a Canadian and international context in a more comprehensive manner; and *iii*) to seek informed contributions to public security policy.

372. Cf. www.cata.ca/files/PDF/homelandsecurity/rapport_canada.pdf. This initiative also involves the development of a database of more than 700 advanced technology companies in the advanced security industry in order to promote new commercial opportunities and partnerships for Canadian based enterprises. The project was backed by the Government of Canada (Industry Canada and Foreign Affairs), the Government of Quebec (Treasury Board) and key players from the private sector (Bell, LGS an IBM company, BMO Financial Group etc), and was assisted by the Canadian Commercial Corporation and several trade associations.

373. "TeleTrusT Deutschland e.V." was established in 1989 as an association dedicated to promoting the trustworthiness of applications and services based on electronic signatures, authentication and encryption, in an open system environment. Cf. www.teletrust.de

374. The T7 association, a working group for digital signatures, was set up in 1999 to combine its members' communication and information activities in Germany and abroad. Cf. www.t7-isis.de/index.html

375. Free versions of the test bed are available from the TeleTrusT office. Cf. www.teletrust.de

The Department of Homeland Security (DHS) in the **United States** works closely with the private sector, academia, and other government agencies to improve software development processes for the production of better quality and more secure software in support of mission assurance. For example, the National Cyber Security Division (NCSD) has hosted and co-hosted various forums and workshops that focus on topics such as the Common Criteria, development of a common body of knowledge for software developers, and improving the quality, reliability, and dependability of software at all levels of assurance. NCSD has also developed a software assurance plan.[376] In April 2004, a Task Force of the "National Cyber Security Partnership"[377] published a report on how to improve security across the software development lifecycle.[378]

h) Technical (including management) standards

Austria has developed the "Austrian Security Handbook"; a compendium for establishing an IT Security Management System (ISMS) and measures for Baseline Protection in organisations, and has created an "E-Government Quality Mark" to serve as a guarantee of a high-quality implementation of e-government applications. To be awarded with the quality mark, such applications, procedures or products must meet defined criteria, *inter alia* with respect to security. The quality mark is aimed at reassuring citizens and the private sector that the respective services and products conform with established standards.[379]

In **Canada**, the ICT Standards Advisory Council of Canada (ISACC)[380] is an industry-government partnership that was formed in 1991. ISACC develops strategic directions for standardisation in the Information Technology and Telecommunications (IT&T) sectors and provides a strategic focus for the development and implementation of Canadian IT&T standards. ISACC accomplishes its work through rapporteurs that monitor, participate and report on all ISACC areas of interest, including IT security.

The National Standards of Canada for IT Security are developed under the authority of the Canadian Standards Association (CSA).[381]

In **Finland**, the CoBit and BS7799 standards are used in information security management. Some organisations in Finland already have BS7799 certificates.

---

376. NCSD's software assurance plan is targeted on the following four areas: *i*)·People – developers (including education and training) and users; *ii*) Processes – best practices and practical guidelines for the development of secure software and standards; *iii*) Technology – software evaluation tools; and *iv*) Acquisition – software security improvements through acquisition specifications and guidelines.

377. Cf. question 8a) above.

378. In the task force, members have considered how to achieve meaningful and measurable vulnerability reductions through collaborative standards, tools and measures for software; new tools and methods for rapid patch deployment; and best-practice adoption across the entire critical infrastructure. The work has included discussion of how to build — and how to teach building — secure software from the ground up, as an embedded and simple feature in all software systems going forward. The task force was comprised of software experts from the vendor, systems integration and end-user communities. The report "improving security across the software development lifecycle" is available at www.cyberpartnership.org/init-soft.html

379. The quality mark is a registered trade mark. It is awarded by the Federal Chancellery, which is responsible for e-government issues. Cf. www.guetesiegel.at (German language).

380. Formerly called TSACC – the Telecommunications Standards Advisory Council of Canada.

381. CSA tasks the Canadian Advisory Committee for Information Technology Security (CAC-ITS) to perform this function. Under the authority of the Standards Council of Canada (SCC), CAC-ITS is also the vehicle for Canada's contribution to international standards development activities.

In **France**, the Central Directorate for Information Systems Security (DCSSI) has developed and promotes the EBIOS risk assessment and management methodology. Furthermore, the DCSSI solicits opinions from the private sector on proposed information system security policies before they are validated. The private sector also participates in the working groups that prepare those policies, via the organisation of State-Industry workshops, through calls for comments over the Internet, and the institution of review committees made up of representatives from trade organisations.

The **German** Federal Office for Information Security (BSI) participates in an international working group for further developing the "Common Criteria" (ISO/IEC 15408). In this context, the Federal Office for Information Security organised the 5th International Common Criteria Conference (ICCC) in Berlin in September 2004. These activities are supplemented by regular workshops the Office has been offering to national audit bodies for several years. At the national level, the "IT Baseline Protection Manual", and a tool for facilitating the implementation of its recommendations, have been developed, together with reference material for the development of information security policies and guidelines. In addition, 12-15 protection profiles (PPs) are currently under development at the Federal Office for Information Security, which are planned to be evaluated and certified in 2005.

The German Federal Ministry of Economy and Labour (BMWA) has conducted a number of standardisation and harmonisation initiatives to promote secure and interoperable services using electronic signatures at the local, national and trans-border levels.[382] Funded by the BMWA, an electronic public procurement application[383] has been launched at the federal level in early 2004, using qualified electronic signatures for legally binding interactions between government and industry to fulfil safety requirements and to foster a culture of security among the parties involved.

Japan is developing a domestic co-operation framework for standardisation of security within ITU-T, and promotes international standardisation of IT security in ISO/IEC, as well as the establishment of Japanese Industrial Standards (JIS) on IT security.

Korea has developed an information security guideline, which forms the basis for mandatory *security check-ups* performed in companies, to strengthen and support the establishment of corporate information security management systems.[384] The Information Security Technology Committee (TC10), under the umbrella of the Korea Telecommunication Technology Association (TTA), has formed three research teams that undertake information security related standardisation work, in which the Korean Information Security Agency (KISA) plays a central role.

In **Norway**, "ICT regulations" have been developed for the financial sector (including banks, assurances, and institutions operating in the security market), audited and overseen by an independent agency ("Kredittilsynet"). Among other things, these regulations address security matters. Furthermore, the project SEID – a co-operation on electronic ID and electronic signatures, was initiated by the Ministry of Trade and Industry, jointly with the then Ministry of Labour and Government Administration (now the Ministry of Modernisation) in autumn 2003. This project was a joint venture with the private sector financed jointly by the participants. It ended in May 2005 and resulted in the development of three industry

382. The Online Services Computer Interface (www.osci.de) specifies the reliable exchange of structured data in e-government business processes. The ISIS-MTT specification (www.isis-mtt.org) defines an interoperability framework for components and infrastructures for electronic signatures and signature cards. The Signature Alliance (www.signaturbuendnis.de), a joint effort of the public and private sectors, negotiates technical and organisational standards to facilitate a coherent market evolution for signature cards and applications.

383. http://evergabe-online.de

384. Cf. www.kisa.or.kr/isms

standards for PKI-interoperability in the Norwegian market which the government is considering to make national standards.[385]

The "**Spanish** Association of Standardisation and Certification" (*Asociación Española de Normalización y Certificación* – AENOR[386]) has developed and published the national standard UNE 71502, the Spanish national implementation of ISO/IEC 17799.

In **Sweden**, Government agencies are involved in information security standardisation initiatives mainly though the Swedish Standards Institute (SIS), for instance in committees and working groups on the SS-ISO/IEC 17799 and ISO/IEC 15408 standards and, regarding smart cards, for example on ISO 7816-15.

In the **United Kingdom**, the predominant trend is the use of the ISO 17799, and of the National British Standard BS 7799 Part 2, a specification for an information security management system.[387]

In the **United States**, the National Computer Security Division (NCSD) in the Department of Homeland Security (DHS) partnered with the Cyber Security Industry Alliance, an industry association, to co-host a two day Common Criteria User's Forum that brought together industry and government stakeholders to discuss the problems with and possible improvement to the Common Criteria. In April 2004, the "Technical standards and Common Criteria Task Force" in the "National Cyber Security Partnership"[388] published a recommendations report addressing standardisation of IT security, and the Common Criteria in particular.[389] Furthermore, the National Institute for Standards and Technology (NIST) interacts with industry in the development of standards and guidelines. All standards and guidelines are published in draft form for comments. NIST also participates in a number of national and international standards bodies.

Portugal plans to address the issue in the framework of its project for a National Information Security Framework, assisting entities in developing their own information security policies, based on the ISO/IEC 17799 standard.

---

385. Preliminary results of the project to date are: the Norwegian qualified certificate profile (SEID-profile) and a common specification for access to the Norwegian Central Population Register, to automatically match a digital signature with the National ID Number of the signer. The last expected result from SEID will be a common standard specification for (long term) storage of digitally signed objects. All SEID specifications / profiles are based on internationally recognised standards, as far as such standards exist and are implemented in the marketplace. The recently published Common Specification for PKI in the public sector in Norway (January 2005) refers to SEID standards in several of its parts.

386. www.aenor.es

387. Cf. question 2d) above.

388. Cf. question 8a) above.

389. The task force pursued a wide-ranging goal with respect to technical standards, and a more focused objective with respect to the Common Criteria. It brought together experts within the private sector and leading research universities to develop new tools, technologies or practices that can reduce vulnerabilities at every level — from the federal government to large and small enterprises and individual home users. The Common Criteria focus has resulted in recommendations for improving the system as it pertains to industry compliance and on how federal agencies can use and implement the system in a more effective way for their own purposes. Cf. www.cyberpartnership.org/init-tech.html

i) Independent certification of the security of information technology

The majority of respondents reported activities with respect to independent certification of the security of information technology. Some respondents made reference to the "Common Criteria" ISO/IEC 15408 standard. Some countries mentioned the ISO/IEC 17799 standard. Some countries apply also national standards for certifying security of information technology products or applications.

Initiative related to the Common Criteria were reported as follows:

Austria has joined the Common Criteria Mutual Recognition Agreement.[390] At the national level, security of information technology is certified by A-SIT.[391]

Canada is actively involved in certification of IT security products using the Common Criteria. The *Canadian Common Criteria Evaluation and Certification Scheme* (CCS) is a Canadian independent third party evaluation and certification service for measuring the trustworthiness of IT security products and systems using the CC.[392] The Canadian CCS establishes "Common Criteria Evaluation Facilities" (CCEF) CSE provides a list of products certified under the CC.

As part of the CSE Industrial Security Program, CSE is also in the process of selecting qualified companies to perform independent system certifications in support of the governments need to certify and accredit systems and services prior to operational use. Canada is also closely monitoring efforts underway within ISO to develop a standard for certification of organisations Information Security Management System (ISMS). To date, no organisations have completed an ISMS certification based on BS 7799 Part 2 in Canada.

In **France**, the *Centre for Information Technologies Security Certification*, a unit of the "*Central Directorate for Information Systems Security* (DCSSI), executes the "information technology security certification scheme".[393] Certification is based on evaluations carried out by laboratories licensed by the French Prime Minister and approved by the French Accreditation Committee (COFRAC) in accordance with the NF EN ISO/CEI 17025 standard.[394] Besides the Common Criteria Mutual Recognition Agreement, France also is a member of the European Mutual Recognition Agreement SOG-IS.[395]

---

390. The Common Criteria Mutual Recognition Agreement provides for mutual recognition of certificates issued by national certification bodies in countries that are parties to the agreement, under the Common Criteria (ISO/IEC 15408), up to CC evaluation level EAL4 incl. In November 2003, the signatory countries to the agreement that issue certificates were Australia, Canada, France, Germany, Japan, New Zealand, the United Kingdom, and the United States. Signatory countries not issuing certificates were Austria, Spain, Finland, Greece, Hungary, Israel, Italy, Norway, the Netherlands, Sweden and Turkey. Cf. www.commoncriteriaportal.org.

391. The "Austrian Center for Secure Information Technology" (A-SIT) is also a notified body according to Article 3(4) of the EU Digital Signature Directive 1999/93/EC. Products certified by A-SIT include secure signature creation devices, smartcard terminals, and secure viewers.

392. CCEF is accredited as an IT Security Evaluation and Testing (ITSET) Facility, under ISO/IEC 17025-1999, and approved by CSE to perform CC evaluations.

393. This includes:. Licensing and supervising information technology security evaluation facilities; supervision of evaluations; analysis of evaluation reports; and issuing of certificates and certification reports.

394. In 2003, the French body for IT security certification issued 25 certificates for smart cards, 3 certificates for software, and 8 certificates for protection profiles.

395. The 1999 SOG-IS European Mutual Recognition Agreement provides for recognition of certificates by all signatory countries issued by certification bodies of any other signatory country. European mutual recognition extends up to the ITSEC E6 and CC EAL7 levels. In April 1999, certificate-issuing signatory countries were France, Germany and the United Kingdom. Signatories not issuing certificates were Finland, Italy, the Netherlands, Norway, Portugal, Spain, Sweden, and Switzerland.

In **Germany**, the Federal Office for Information Security co-operates with accredited auditing bodies in carrying out product evaluations and certifications on the basis of the Common Criteria ISO/IEC 15408.[396] In addition, 12-15 protection profiles (PPs) are currently under development at the Federal Office for Information Security, which are planned to be evaluated and certified in 2005.

In **Japan**, the IPA executes an IT evaluation and certification scheme based on ISO/IEC 15408.

The **Norwegian** *National Security Authority* (NSA) administrates the certification of information systems and products, based on the Common Criteria Standard. SERTIT is the public Certification Authority for IT Security in Norway, and issues Certificates and Certification Reports.[397]

In **Sweden**, the Defence Materiel Administration Certification Body will soon be operational with a Swedish scheme for evaluation and certification of IT security using the Common Criteria.[398]

In the **United States**, the National Institute for Standards and Technology (NIST) facilitates and participates in international certification recognition arrangements, and assists with Common Criteria (CC) evaluation and validation programmes.

Activities based on the ISO/IEC 17799 standard were reported from the following respondents:

Institutions in the government in **Denmark** are required to implement an IT security standard based on national implementation of the ISO/IEC 17799 standard (DS 484).

Finland reports CoBit and BS7799 to be the standards used in information security management in the country. Some organisations in Finland already have BS7799 certificates.

Norway has established IT security certification schemes for implementation in organisations based on the standard NS-ISO/IEC 17799, under the supervision of Norwegian Accreditation (*Norsk Akkreditering*).

Portugal plans to address the issue in its project for a National Information Security Framework, assisting entities in developing their own information security policies, based on the ISO/IEC 17799 standard.

In **Spain**, the "Spanish Association of Standardisation and Certification" (*Asociación Española de Normalización y Certificación* – AENOR[399]) certifies information security management systems under the Spanish national implementation of ISO/IEC 17799 (UNE 71502).

---

396. Cf. www.bsi.de/cc/index.htm. Around one fifth of the approximately 100 common criteria IT security certificates issued world-wide in 2003 were issued by the German Federal Office for Information Security (plus ca. 30 in 2004), cf. www.bsi.de/zertifiz/zert/index_en.htm. An up-to-date list of the CC certificates issued world-wide is available via the "Common Criteria Portal" at www.commoncriteriaportal.org.

397. Companies that want to join the Scheme as an IT Security Evaluation Facility (ITSEF) have to be approved by SERTIT. The management of ITSEF and the evaluation process is carried out under supervision of SERTIT, which is also representing Norway in the "Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security (CCRA)".

398. Cf. www.csec.se (Swedish language) and www.fmv.se/default.aspx?id=121 (Web site of the Defence Materiel Administration, in English).

399. www.aenor.es

National standards or similar instruments are used in the following countries:

In **Austria**, the "Austrian Center for Secure Information Technology" (A-SIT) is accredited as an inspection body for electronic payment systems and for compliance with the Austrian Security Handbook.

The Federal Office for Information Security in **Germany** provides a certification mechanism based on the German IT Baseline Protection Manual through licensed auditors.[400]

In **Japan**, the Ministry of Economy, Trade and Industry (METI) promotes an Information Security Management System (ISMS) certification scheme for the private sector.

In **Korea**, in the framework of the "Act on Telecommunication Network Usage Facilitation and Information security", the information security management systems operated by companies are being audited since 2002. A certificate is issued according to the result of the inspection.[401] Furthermore, to strengthen regular security activities and to support the establishment of information security management systems, Korea has made it mandatory for companies to undergo a "security check-up", based on an information security guideline. Korea has also developed and published evaluation criteria for firewalls (1998) and intrusion detection systems (2000) applicable to the national information security product evaluation and certification system.

Norway has for the financial sector (including banks, insurances, and institutions operating in the securities market) a set of "ICT regulations" in place, which *inter alia* address the security of IT systems operated by such institutions in the country. Adherence to the regulations is audited on-site by an independent government agency ("Kredittilsynet"), based on the CoBiT methodology, at a number of institutions subject to the regulations each year. *Kredittysilnet* also issues an annual sector-specific risk analysis report.

In the **United Kingdom**, the use of third party assessment against the national British standard BS 7799 Part 2 is increasing steadily and it is expected to further increase significantly if and when the standard forms the basis of a new ISO standard in late 2005.

In the **United States**, vendors of cryptographic modules and algorithms use independent private sector testing laboratories accredited as Cryptographic Module Testing (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP) to have their cryptographic modules tested by the Cryptographic Module Validation Program (CMVP) and their cryptographic algorithm implementations validated by the Cryptographic Algorithm Validation Program (CAVP). The CMVP and the CAVP are collaborative programs between the NIST Computer Security Division and the Communication Security Establishment (CSE) of the Canadian Government to provide Federal agencies – in the United States, Canada, and the United Kingdom – with confidence that a validated cryptographic product meets a claimed level of security and that a validated cryptographic algorithm implementations have been implemented correctly.[402]

---

400. This service was introduced in 2003. At present, *ca*. 100 auditors are licensed all over Germany to conduct such audits. By the end of 2004, *ca*. 10 certificates had been issued under this certification system. Cf. www.bsi.bund.de/gshb/index.htm (German/English).

401. Cf. www.kisa.or.kr/isms. It is planned to facilitate the certification system in 2005, and to improve the criteria, and the overall level of examination.

402. The CMVP validates modules used in a wide variety of products including secure Internet browsers, secure radios, smart cards, tokens, and products supporting Public Key Infrastructure and electronic commerce. Statistics from the testing laboratories show that out of the first 200 modules tested, 48% of the

Other initiatives were reported as follows:

In the **United Kingdom**, the Government has developed a new approach based on a "claims tested" mark for advising users about the effectiveness of information security products which requires much less expensive evaluation.

No initiatives have been reported for questions 8a)-8i) above from the **Czech Republic**, and the **Slovak Republic**.

V. Government as partner with civil society[403]

Question 9: Most successful government collaborative initiatives with, and outreach initiatives to, civil society to promote a culture of security for information systems and networks among users (including households and the general public). Initiatives currently being developed and/or respective plans for the future.[404]

Austria aims at encouraging its citizens to use new, more secure technologies by making available a new ATM card, a Health Insurance Card (the eCard), and a "mobile electronic signature".[405] It is also expected that electronic government and a new form of online banking with electronic signatures will not only raise awareness, but also establish a higher level of security. An "E-Government Quality Mark" has been created, awarded to e-government solutions that fulfil certain defined quality criteria, including security.[406]

The Office of Consumer Affairs within Industry **Canada** has developed a gateway to all of the information and services offered by Canada's governments and NGOs. The Canadian Consumer Information Gateway is a partnership between 400 federal departments and agencies, provincial and territorial ministries and NGO partners that allows Canadians to search for consumer information and services on the Internet. The Gateway offers an array of publications, tip sheets, and information sources on Internet safety and security such as:

- Protecting Your Financial Privacy in Cyberspace (Alberta - Better Business Bureau of Central and Northern Alberta).
- Stop Spam Here (Industry Canada).
- Theft of Telecommunication Services (Royal Canadian Mounted Police).
- Protect Yourself Against Identity Theft (Canada's Association for the Fifty-Plus).

---

cryptographic modules and 27% of the cryptographic algorithms brought in for voluntary testing had security flaws that were corrected during testing. In other words, without this program, the Federal government would have had only a 50/50 chance of buying correctly implemented cryptography. To date, over 460 certificates have been issued for validated modules by the CMVP, representing over 120 vendors. Likewise, over 1 312 certificates have been issued for validated cryptographic algorithm implementations. Over 336 of these certificates were issued in 2004.

403. This section was meant to address both the policy-oriented principles (1-5) and the operation-oriented principles (6-9) of the 2002 *OECD Security Guidelines.*

404. Including a discussion of the foreseen division of responsibility between government, civil society and the private sector (businesses).

405. For a detailed description of these projects, *cf.* the answer from Austria to the questionnaire.

406. Cf. question 8 h)

- Principles of Consumer Protection for Electronic Commerce (Industry Canada).
- Web Watchers Tips (Marketplace).

Development of the tools is ongoing.[407]

In the **Czech Republic**, the National Program of Computer Literacy (NPCL) is aimed at providing beginners with the basic computer skills. NPCL was launched by the Ministry of Informatics in February 2003. The project implementation is based on public private partnership principles, *i.e.* on co-operation of public and private sectors,[408] and is expected to be expanded to also cover information security in the future.

In **Denmark**, civil society is targeted through awareness campaigns and information material.

In **Finland**, the Data Protection Ombudsman has drawn up instructions for citizens to promote and improve data protection. The Office of Data Protection Ombudsman has included several practical means for safeguarding data protection in their guidebook.[409] As a part of the national information security strategy, a broad co-operation team consisting of both governmental and private bodies was established for setting up a *National Information Security Day*, an annual event held in February. It is organised jointly by various public-sector bodies, private-sector businesses and other organisations to increase awareness of current threats to information security and practical measures of protection against these threats.[410] Finland has also set up an interactive online government discussion forum for citizens and other participants.[411] The Ministry of Finance has used this forum for interactive online discussions about information security with citizens. Information security professionals from the government, such as members of the Government Information Security Management Board (VAHTI), also have participated actively in these discussions, for example.

France has to date not launched a wide-scale public awareness-building campaign. However, information from some government institutions is available to the general public on the Internet.[412] In

407. Cf. http://consumerinformation.ca

408. The aim of the initiative to date is to provide the general public with the opportunity to acquire basic computer and Internet skills for affordable fees. 25 000 participants have completed this course within ten months. The training centres network grew up to 240, in 145 cities and towns in the Czech Republic. The biggest interest in the programme was shown by persons between 40 and 60 years of age. Women account for 60% of participants. As a follow up, courses will be targeting more specialised issues, where information security could be a part.

409. In addition, the "Mannerheim League's" Netsmart guidelines are especially targeted at children and their parents. They have been designed to combat risks to children as users of the Internet, in collaboration with other institutions, *e.g.* the National Council for Crime Prevention.

410. The first national information security day was held on 11 February 2004. The main focus of that day was on end users, *i.e.* individual citizens. The aim of the first National Information Security Day was that everyone with a home PC linked to the Internet would ensure that their operating system would have the latest information security updates, current anti-virus software and a firewall. The second information security day was held on 8 February 2005, with the main focus on students in comprehensive schools, and with the main goal to give guidance for students and their parents on information security issues in general and on how to use Internet in a secure way. Cf. the general Web pages on the information security day at www.tietoturvaopas.fi/, and the specific site set up for the 2005 information security day at www.tietoturvakoulu.fi/ (both Web sites available in Finnish and Swedish).

411. www.otakantaa.fi

412. Cf. www.ssi.gouv.fr and www.telecom.gouv.fr/secur/index.htm.

addition, various business associations have also published, or are in the process of preparing studies on the subject.[413]

In **Germany**, a "quality mark monitoring board" has been set up to support suppliers in selecting a quality mark and in drawing the Internet buyers' attention to such quality marks. For this purpose, the "Initiative D21" has developed appropriate quality criteria for online offerings in co-operation with the Federal Ministry of Economics and Labour and the German Working Group of Consumer Associations (*Arbeitsgemeinschaft der Verbraucherverbände*). The Monitoring Board of the quality mark suppliers works on the further development of the D21 quality criteria and monitors all the recommended suppliers for compliance. Members of the board are representatives from quality mark suppliers, Initiative D21, the Federal Data Protection Commissioner, consumer and industry associations, as well as other experts.[414] Other projects of Initiative D21 for the civil society include: *i*) *Jugend ans Netz* (Youths to the Net), *ii*) the "Ambassador Programme", *iii*) online competence for generation 50plus, *iv*) e-skills in business and administration, and *v*) promoting acceptance of the electronic health insurance card.[415] Additional initiatives by the federal government include awareness campaigns and services offered by the Federal Office for Information Security to private households and the general public,[416] and a government-funded project on technical and regulatory foundations of e-voting.[417]

In **Japan**, the "MIC Information Security Site for the People" has been launched in March 2003.[418] In addition, the Japanese Ministry of Economy, Trade and Industry (METI) holds regular seminars on countermeasures against computer viruses and unauthorised access for general IT users in nationwide collaboration with non-profit organisations (NPO). The Information Technology Promotion Agency (IPA) and the Japan Computer Emergency Response Team Co-ordination Center (JPCERT/CC) regularly hold seminars across the country on countermeasures against computer viruses and unauthorised access, aimed at managers of information systems. Furthermore, the National Police Agency (NPA) convenes similar seminars in various cities in Japan, in co-operation with non-profit organisations. The NPA, together with the prefectural police, has made an integral effort in prevention and investigation of cybercrime.[419] Finally, the NPA security portal site '@police' provides content on the safe use of the Internet for children, 'Security Online Lectures' and 'Security Easy-diagnosis', with technical advice for Internet users.

413. Cf. *e.g.* www.clusif.asso.fr and www.cigref.fr

414. Cf. www.Internet-guetesiegel.de

415. Cf. www.initiatived21.de, and the description of the projects in question 10.

416. Cf. question 8a).

417. Since 2000 the German Federal Ministry of Economy and Labour (BMWA) has funded a project on technical and regulatory foundations of eVoting. The pilot platform has been used for several test polls (*e.g.* for the D21 board, the Deutsche Telekom staff council, and the students parliament University Osnabrück), and aims at a commercial market for board elections of associations and enterprises. The software is currently undergoing a major redesign.

418. www.soumu.go.jp/joho_tsusin/security/index.htm

419. This includes joint PR activities to prevent cybercrime, in co-operation with other relevant organisations, and the investigation of Web sites with illegal or harmful content flagged by the general public.

Korea has put in place an annual "Information security week" (in the third week of June), and organises a number of relevant events to raise public awareness on the importance of information security.[420] In addition, it is planned to organise an "Information security Award", designed to reward organisations such as companies and universities that have a good information security level, and improve the overall level of information security in the private sector. Finally, a number of workshops have been organised to share the latest information on key issues, policy and technology of information security.

In the **Netherlands**, the most successful initiatives with outreach to civil society include *Surf op Safe*, the *Alerting Service*, *KWINT*,[421] *DigiD*, and *the Burger Service Nummer*:

DigiD is a collective system of and for the Dutch government (www.digid.nl) for once-only provision of username and password for electronic services. With this information, the government can verify the identity of the user of electronic services. The login information enables the user to access a growing number of government services on the Internet. It is expected that the number of connected e-government organisations (as of March 2005, a number of municipalities and the Center for Work and Income - CWI) will increase rapidly in the near future.

The *Civil Service Number (Burger Service Nummer)* will introduce a personal number for Dutch citizens, to be used for identification in contacts between citizens and the government. This number is one of the instruments to achieve a once-only provision of personal information to government organisations, and the streamlining of registration of basic information. The introduction of the personal number is planned for January 2006, under the responsibility of the Ministry of the Interior.

Norway launched a new Web site (www.nettvett.no) in April 2005 to raise awareness and increase knowledge in the field of information security. The target groups are primarily consumers and individual enterprises.

Portugal is planning to create security guidelines for citizens on how to securely use a PC, as part of its project for a National Information Security Framework, intended to be adopted by National Public Administration, the private sector and civil society.

In **Spain**, the Directorate-General for Information Society Development has supported successive awareness campaigns for information security, organised by the Internet Users Association in collaboration with industry, with explanatory material on security problems made available on the Internet. Up to now, four campaigns have been developed: *i*) a Web site for the general public with instructions, recommendations and free software tools on information security ("CAMPAÑA DE SEGURIDAD EN LA RED") has been promoted to the general public in Spain through co-ordinated information via traditional mass-media; *ii*) the "Center for Early Alert on Viruses and Computer Security" (http://alerta-antivirus.red.es), operated by Red.es,[422] provides Internet users with free, detailed information on viruses, up-to-date alerts and a back catalogue of previous virus alerts. Subscription to free periodic reports, and to a free newsletter with alerts and information about viruses are also available. The site offers general information on computer security, on vulnerabilities, as well as security patches and updates of software, discussion forums and an expert consultation service; *iii*) Red.es has also designed a "Safe Navigation"

420. Including the declaration of an "action plan for information security", as well as the organisation of a "Contest for Information security Slogan and Poster," a " Hacking Response Challenge" (where security experts write a hacking analysis report)," a "Street Campaign for Information security," and a "Safe PC Campaign", where vaccine programs are offered for free download.

421. Kwetsbaarheid op Internet (KWINT); cf. question 8a) above.

422. Red.es (cf. www.red.es) is a Public Enterprise assigned the Secretariat of State of Telecommunications and for the Information Society, in the Ministry of Industry, Tourism and Commerce.

site, to increase confidence of adults and children in the Internet;[423] *iv*) another Web site has been explicitly dedicated to children.[424]

The **United States** has set up a *National Cyber Alert System* (NACS), an operational part of the US-CERT Response System that delivers targeted, timely, and actionable information to users to allow them to secure their computer systems. The alert system targets all levels of computer user sophistication, from the technical professional to the non-technical home user, reflecting the broad usage of the Internet in today's society. Launched in January 2004, the alert system also offers the operators the possibility to reach millions of users at one time. More than 270 000 users have subscribed to the system and receive regular alerts and updates.[425]

Furthermore, the Federal Trade Commission has for years partnered with consumer and technology groups to expand its distribution of print and Web publications on topics related to information security. The FTC maintains ties and actively works to promote consumer education with these organisations through coalitions like the *Alliance Against Fraud in Telemarketing and Electronic Commerce*, *National Cyber Security Alliance*, *Anti-Phishing Working Group*, and others. In 2003, the FTC co-ordinated the fifth annual National Consumer Protection Week with a consortium of public- and private-sector organisations around the theme of information security. The initiative's Web site[426] offered a poster featuring the mascot "Dewie" and information security themes, and included a link to the FTC information security Web site.[427] Numerous organisations, including nine on the steering committee of the event, packaged the available information in meaningful ways for consumers and distributed it nationwide.

Australia, the **Slovak Republic** and the **United Kingdom** have not indicated activities in this domain.

Question 10: What were the most successful government initiatives in the education system in your country (pre-school age, all school ages, and higher education) to address the culture of security? Are such initiatives currently being developed or are there any plans for doing this in the future?

In 1999, **Australia** created "Net Alert",[428] an advisory board to promote a safer Internet experience, in particular for young people and their families. Net Alert works closely with the European Internet Safety Network (Insafe) and uses the media to announce its initiatives, including a toll-free national help-line and e-mail advisory service, an education campaign, regional forums and advertising campaigns, information resources and a programme to advise the Internet industry of its rights and obligations under the government's online content regulatory scheme. In addition, in 2004 Net Alert launched the CyberSafe Schools initiative which aims at providing primary and secondary schools' teachers with appropriate material to deliver education programmes, and Netty's World, a Web site for young children starting out on the Internet. In 2004, most initiatives were launched on the Safer Internet Day.

---

423. Cf. http://navegacion-segura.red.es. On this site, parents and children can surf the Internet without running the risk of encountering illicit or inadequate content. The site *i.a.* offers advice to parents, to enable them to educate their children in using the Internet. It also contains information on tools like filters, *i.e.* computer programs that serve to protect children from inadequate content.

424. Cf. http://chaval.red.es. The site offers links to educative and leisure content recommended for children of 6 to 12 years, previously checked by experts.

425. Cf. www.us-cert.gov/cas/

426. www.consumer.gov/ncpw2003

427. Cf. www.ftc.gov/infosecurity

428. www.netalert.net.au

Since 2000, **Austria** has been working on signature cards for students and scholars. Since 2001, cards have been introduced in some Universities for uses such as ID-card, authentication, electronic signature, room access, copy card and electronic wallet. The cards can also be used in e-government and are part of the citizen card concept. Similar cards are currently introduced in ten pilot schools, and the government is working on the issue of technical interoperability with federal applications.

In **Canada**, the SchoolNet,[429] a public (federal, provincial) private partnership launched in March 1999, connected Canada's schools and public libraries to the Internet. As of May 2000, half a million computers were connected in Canadian schools. Many educational institutions have developed policies addressing the security of information systems and networks. Examples include the University of Ottawa which developed a Policy on Electronic Data Processing (EDP) Security, and a Policy on University Wireless Communications.[430] The Ottawa-Carleton District School Board (overseeing 150 elementary and secondary schools) has adopted a policy on computer network security.[431]

In **Finland**, the National Board of Education gave instructions to schools about secure use of the Internet and provided schools with information security material from the Ministry of Finance. It launched the DotSafe[432] pilot project to provide educators and parents with material to teach children how to stay safe on line. DotSafe is a pilot across the 23 member countries of the European SchoolNet. The 2005 National Information Security Day[433] (8 February) focused on information security in schools with the objective of giving guidance to students and their parents on information security issues in general and on how to use Internet in an information-secure way.

The **French** government has as yet not launched any specific initiative in schools. The government's Information System Security Training Centre (CFSSI) has published a study on cyber-security education programmes in public universities[434] and maintains a list of information security courses in France.[435]

In **Germany**, the Federal Ministry of Education and Research supports the "Schools go online"[436] initiative, a nation-wide competence centre for teaching and learning to use new media at schools, and for providing teachers with educational material related to information security. The "Youths to the Net"[437] initiative aims at reducing the digital divide through providing secure and pedagogically controlled access to the Internet for children and youths. The Federal Office for Information Security supports students writing a thesis at scientific institutions. In 2004, a thesis on steganography won the first prize of the Competence Centre for Applied Security Technology (CAST).[438] Finally, the Initiative D21 aims at fostering basic knowledge on Internet use, including security aspects, among citizens aged over 50.[439]

429. www.schoolnet.ca

430. http://Web5.uottawa.ca/admingov/reg-e.php?id=45

431. www.ocdsb.edu.on.ca/Policies_Procedures/Policies/P%20074%20IT%20Comp%20Net%20Secur.pdf

432. www.dotsafe.eun.org and www.edu.fi/dotsafe

433. www.tietoturvaopas.fi and www.tietoturvakoulu.fi (in Finnish and Swedish)

434. www.formation.ssi.gouv.fr/formation/superieure/

435 . www.formation.ssi.gouv.fr/formation/superieure/formfrance.html

436 "Schulen ans Netz", www.lehrer-online.de/url/it-sicherheit

437. "Jugend ans Netz", www.jugend.info

438. www.bsi.bund.de/presse/pressinf/251104_cast.htm

439. www.50plus-ans-netz.de

Korea organised a National Training Tour from March to November 2004, aimed at raising awareness on information security and educating the public as to how to protect their computers, and training system managers. Korea has also published a cartoon booklet to prevent children from Internet addiction and plans to publish a textbook and gaming software on information security for elementary school students.

In the **Netherlands**, children are a special target group of the "Surf op Safe" campaign. The "Diploma Safe Internet" campaign educates children between 8 and 12 about how to manage risks on the Internet. Children can take an exam and receive a diploma if they succeed. Through another initiative launched in 2002 together with various other stakeholders, courses are offered to parents of young children to inform them about security risks. Cyber Secrets[440] is a course with practical exercises and education material which can be used in schools. It targets children from the upper elementary grades to the upper end of secondary education. Finally, the Internet provider of higher education and many research organisations in the Netherlands maintains the SURFnet-CERT which handles all cases of computer security incidents involving their customers and also provides alerts and advisories.

In **Spain**, the FORINTEL[441] initiative of the General Direction for Information Society of the Industry, Tourism and Commerce Ministry includes security in its basic Internet education programmes.

In the **United States**, the National Centres of Academic Excellence in Information Assurance Education (CAEIAE) program has been extended to the national level in 2004 through an agreement between the Department of Homeland Security (DHS) and the National Security Agency (NSA) with the aim of developing a larger cyber security work force to support both the public and private sectors. DHS also partnered with the National Science Foundation in March 2004 to co-sponsor the Scholarship for Service (SFS) program "Cyber Corps". This program provides scholarship grant money to selected CAEIAE and universities to fund the final two years of students in information assurance. Three hundred students participate in the program every year and agree to work for a federal agency for two years.

In addition, the Federal Trade Commission (FTC) developed a Web-based safe-surfer quiz.[442] It partners and shares publications with, and links to many other organisations on its security information Web site in order to promote a culture of security among school-age children and consumers of all ages.[443] The FTC also distributed 160 000 postcards featuring Dewie the turtle to 400 college campuses in the United States.

The **Czech Republic**, **Denmark**, **Japan, Norway, Portugal** the **Slovak Republic** and the **United Kingdom** reported no activities in this area.

440. www.kennisnet.nl/thema/cybersecrets/

441. www.forintel.es

442. www.ftc.gov/bcp/conline/edcams/infosecurity/popups/safesurf_quiz.html

443. www.ftc.gov/infosecurity

VI. Government efforts related to S&T and R&D

Question 11: Science and Technology (S&T) and Research and Development (R&D) activities underway (or planned). [444]

In **Australia**, issues of information security and critical infrastructure protection have been recognised as an R&D priority, and are funded by the Department of Education, Science and Training.

Austria has several R&D activities in the information security domain. Funded by the Austrian Federal Ministry of Transport, FIT-IT,[445] a EUR 8 million research programme is tailored to support projects in the ICT area. Moreover, innovative information security-related projects are funded through the FWF,[446] the country's main scientific grant institution. Another active body is the Austrian Research Promotion Agency Ltd. (*Österreichische Forschungsförderungsgesellschaft*), whose objective is to promote research among enterprises and research institutions. Individual researchers are also invited to submit proposals. This agency, moreover, supports co-operation between industry and academics, as well as with other international partners, and provides assistance for the participation of Austrian research institutions within European research initiatives.

Canada's Communication Security Establishment (CSE) is a federal government agency delivering information technology security solutions to the government. It has developed several methodologies to determine network security requirements. CSE has also funded a risk assessment project providing a harmonised approach to risk management, the *Guide to Risk Assessment and Safeguard Selection of Information Technology Systems*. Similar efforts have been made in the area of security management, and for certification and accreditation.

The CSE is also active in developing and promoting standards through its involvement in the Standards Council of Canada and the International Organisation for Standardisation (ISO). Finally, together with Public Works and Government Services Canada, it is leading the ITS Product Pre-qualification Programme, aimed at facilitating the government's procurement of products and services. A similar initiative has been put forward for cryptographic solutions and services.

In **Denmark** current research activities focus on information security management, with benchmarks and metrics to be tackled soon. Particular attention is currently paid to the implementation of the DS 484 information security standard within government institutions. Finally, there is an open dialogue between private and public sectors in this domain, including participation in conferences.

Finland has various R&D activities underway under its different information strategy projects.

In **France** the Directorate-General for Enterprises in the Ministry of Economics, Finance and Industry, launched several calls for information security-related R&D projects as part of the Oppidum research initiative in 2001-2004. This programme funds research projects aimed at tackling complex information security-related issues such as digital identity, secure electronic transactions, networks and terminal equipment. The same ministry also provides funds for projects undertaken with industrial and

444. Possible areas listed in the questionnaire as examples in which government may have S&T and R&D activities were: vulnerabilities; best practices; security standards; development of secure software (*e.g.* methodologies); benchmarks and metrics for measuring the security of information systems and networks and the impact of respective initiatives; other.

445. Research, Innovation, Technology - Information Technology.

446. *Fonds zur Förderung der wissenschaftlichen Forschung*.

technological research networks, and supports a number of projects relating to security systems, software and components.

Germany's Federal Ministry of Education and Research supports several information security research activities. In 2003, it funded a two year project aimed at developing methods and tools for formal verification of integrated computer systems with a total sum of EUR 7.6 million. This initiative, called VERISOFT, is co-ordinated by Saarland University. Another EUR 2.4 million were allocated to the MIND project, involving researchers from the Fraunhofer Institute, Siemens, IT Service OMNIKRO and the St. Petersburg-based Institute for Information and Automation, to develop new methods for detecting and preventing intrusions into computer systems connected to the Internet. The Ministry is also supporting the SICARI initiative aimed at developing secure tools and architectures for ubiquitous computing with EUR 5.6 million. This initiative brings together several research institutions and commercial organisations like Philips and T-Systems. Furthermore, the German Federal Ministry for Economics and Labour (BMWA) has funded the "VERNET" programme to support the development of IT security in e-business,[447] and a project for mobile citizen services ("Mobile Bürgerdienste" – MoBüD), an application for secure mobile access to e-government services.[448]

The Federal Office for Information Security (BSI) hosts several studies and development projects in co-operation with industry, for example, on penetration testing, early warning, biometrics, cryptography, RFID, e-government and trusted computing. The BSI is also active in the Trusted Computing Group. Finally, the Federal Criminal Police Office undertakes research in areas like biometrics, ID documents, and visa, together with BSI and other research institutions.

Japan indicates that research activities are currently being undertaken in the areas of implementation of technologies to prevent and detect vulnerabilities, advanced network authentication, cryptographic technology, time stamp and over system security and reliability. R&D activities in the areas of information security are an important element of the **E-Japan** Priority Policy Programme, including analysis of technologies for the prevention and detection of cyber-terrorism, infrastructural technology, authentication, cryptography and time stamping. Several of these projects are undertaken within the Information Technology Promotion Agency and its IT Security Centre.

The **Korean** Information Security Agency is actively involved in information security R&D activities. It is currently conducting joint research activities with US counterparts in order to develop systems for automatically analysing vulnerabilities and provide automated responses. It is also developing and disseminating software to detect Web site vulnerabilities. The Korean Government also develops information security infrastructure technologies through its subsidiary research institutes, and plans to commercialise them after incorporating the needs from the private sector. Furthermore, to develop an information security technology standardisation model, the Korean Government plans to train experts in international standards, who would actively work with international standardisation organisations such as ISO and the ITU.

The **Netherlands'** information security R&D activities have recently been independently evaluated. The final report of this evaluation concluded that Dutch information security R&D activities focused on

447. In VERNET (Safe and Reliable Transactions in Open Communication Networks: www.vernetinfo.de) security technologies are developed, tested and demonstrated in order to increase the acceptance of new media and e-Commerce. Examples of best practice applications are: Long-term conservation of provability of electronically signed documents – ArchiSig, Security Technologies for Internet Metering – Selma, and a VPN-Architecture based on Mikrokernel-Based Operating Systems -µSina.

448. MoBüD is part of the MobilMedia R&D programme (www.mobilmedia.de) The project results will be used by the State of Berlin and the City of Magdeburg.

certificates, software security, security tools, organisation and secure e-government. These projects involve both universities and research centres of commercial organisations. Moreover, the report emphasises the increasingly multidisciplinary approach of Dutch research activities in the field of information and network security.

In 2004, the Ministry of Economic Affairs, the Netherlands Organisation for Scientific Research and the Technology Foundation launched the Sentinel Research Programme. The goal of this initiative is to boost the country's information security capabilities. The programme is to last until 2012 and has a budget of EUR 10 million.

The Research Council of **Norway** supports information security research through the IKT SoS initiative. Universities and research institutes are the beneficiaries of this programme and co-operation with industry is supported. The objective of the programme is to fund single projects or a total portfolio of projects that are expected to be of importance for the security of Norway's commercial organisations and government institutions. In particular, this initiative aims at finding solutions to enhance the overall competitiveness of the country, as well as specific knowledge in the field of information security. The IKT SoS was launched in 2003 with a five-year duration, and a total budget of EUR 7 million (NOK 59 million).

Norway is also supporting the project BAS5 Critical Information Protection. The objective is to develop a methodology to analysis vulnerabilities in critical information protection and develop a ranking methodology to rank critical systems and sectors. The project employees also use novel methodologies in critical infrastructure protection such as scenario analysis and interdependency matrices.

The **Slovak** Ministry of Post and Telecommunications has recently co-ordinated a study on security standards and overall security issues.

Through the "Profit" programme, **Spain's** Ministry for Education and Science supports research activities undertaken by business and research institutions in the areas set by the Spanish National Scientific Investigation Plan. Under this programme, the Ministry of Industry, Tourism and Commerce has established a specific action line to address security concerns. Within Profit, it is possible to finance projects specifically aimed at the development of applications and innovative services for information management. In this context, information security is seen as an important element to address and develop.

In **Sweden** the Swedish Emergency Management Agency (SEMA) has the responsibility to co-ordinate research and development programmes within the information assurance area. SEMA is financing research projects on information assurance, which have to be of relevance to the needs for knowledge defined in the strategic risk assessment. Within the CIP area, research initiatives are financed by SEMA, for example, on strategic CIIP and the connection between threats and planning of counter measures. This initiative also covers areas such as Civil Contingencies and Emergency preparedness. Another research programme covers Computer Network Attacks and International Humanitarian Law. Finally, SEMA is also financing research programmes in cyber terrorism.

R&D activities reported from the **United Kingdom** include research projects on cryptography (including quantum and elliptic curve cryptography), quantum-secure digital signatures, intrusion detection systems, security in mobile computing, analysing data gathered on attack attempts through "honeynets", and detecting and preventing criminal activities on the Internet such as denial-of-service attacks. All projects reported are funded through the Engineering and Physical Sciences Research Council (EPSRC), the UK Government's leading funding agency for research and training in engineering and the physical sciences. Some have additional funding from other sources, notably from private companies. In addition,

UK organisations and companies take part in a wide range of EU research activities funded under the EU framework programmes.

The Science and Technology Directorate (S&T) of the **United States'** Department of Homeland Security is responsible for prioritising and implementing the Department's research and development programmes. The National Cybersecurity Division (NCSD) works with S&T to identify and co-ordinate cyber security and critical infrastructure protection R&D priorities.

The White House Office of Science and Technology Policy has introduced a Critical Information Infrastructure Protection Interagency Working Group (CIIP IWG) as part of the National Science and Technology Council. The Director of Cyber Security R&D in the DHS S&T Directorate co-chairs this group, which brings together 20 organisations from 11 departments and agencies, and several White House offices. The CIIP IWG is currently developing R&D plans in response to the National Strategy to Secure Cyberspace and the Homeland Security Presidential Directive. The NCSD actively participates in CIIP IWG activities and continues to identify critical cyber R&D requirements in co-ordination with the other divisions, for incorporation into all federal R&D planning efforts, including the Federal Plan for Cyber Security Research and Development. NCSD has also contributed to the development of the National R&D Plan for Critical Infrastructure Protection. In addition, the National Institute for Standards and Technology (NIST) continues to undertake research initiatives in complex information security domains.

The **Czech Republic** and **Portugal** have not indicated activities in this domain.

VII. Metrics and benchmarks

Question 12: Metrics and/or benchmarks for measuring the impact and/or success of government's activities for Sections I-VI. [449]

In **Austria** studies have been launched to measure the uptake of the government initiatives. In April 2003 the Ministry of Economics and Labour invited Austrian IT users and suppliers to join a competition by submitting examples of how digital signatures have added substantial benefit (*e.g.* enhanced security) to electronic processes.

In **Canada**, federal departments are expected to conduct active monitoring and internal audits of their security programmes and report the findings to the secretariat of the Treasury Board of Canada. According to the findings of the last exercise, less that 50% of the departments had audited their IT security programme. These results have provided an incentive for requesting government departments and the Treasury Board to put forward an annual schedule of IT security monitoring activities. Moreover, the Chief Information Officer Branch of the Treasury Board Secretariat has developed a self-assessment questionnaire for federal departments about security policies and practices.

Denmark has developed benchmarks to measure the level of security culture, based on a set of common indicators.[450] Related questions are part of the questionnaire of the countries' annual ICT statistics. This publication serves as a baseline for developing new strategic policies.

449. Related principles of the *OECD 2002 Security Guidelines* for this question are: Security management, Reassessment.

450. The following indicators are being measured: It-security among population (loss of data in connection with computer-virus attack, credit card fraud, abuse of personal information, spam, unjustified money collection, level of virus infections, other security problems); It-security countermeasures among population (installed anti virus software, updating anti virus software, using Web pages with password or the like, installed firewall, fear of using credit cards in online transactions, reluctance to send personal and

In **Finland**, the National Information Security Advisory Board has called for monitoring of the implementation of the Finnish National Information Security Strategy. The development of indicators is a specific project within the strategy, and indicators are also being developed to assess the impact of specific projects and initiatives detailed in the strategy.[451] The Ministry of Finance has funded a common government project for the development of metrics and benchmarks, expected to be completed in 2005.

In **Germany** several methods and processes have been put in place to check and verify the level of IT security within systems, and the overall effectiveness of the Federal government initiatives. The Federal Ministry of Education and Research (BMBF) regularly assesses funded research activities. The Federal Office for Information Security (BSI) carries out polls to assess the level of awareness about its products and services among data protection commissioners and trade journalists. Moreover, a survey of the awareness of the general public for information security was completed in 2004. Polls among experts and citizens are also planned for the future.

Japan is currently putting in place a procedure to assess and monitor the implementation of its e-Japan Priority Policy Programme. Moreover, the government has also established a "Committee for Information Security Governance" in September 2004. This body is currently working on an integrated evaluation framework that includes a set of security indicators. A first set of results from this effort is expected to be completed by the end of 2005.

In **Korea** the government applies the management by objective (MBO) methodology in the development of its information security policy initiatives. The results of information security policies are evaluated by determining whether the proposed goals, either qualitative or quantitative, were accomplished or not. Typical indicators include, for example, the number of times spam relays were tackled, the number of security diagnosis services performed, the number of information security education courses and the number of participants in such courses, the number of information security technology standardisations achieved, and the number of information security system evaluations.

In the **Netherlands** there is no central organisation with the responsibility of developing metrics and benchmarks. This is devolved to individual institutions. The VISTIC (Critical Information Infrastructure) project is presently being evaluated. Other initiatives such as Govcert.NL and PKI for Government are also regularly monitored and evaluated. In addition, the Ministry of Economic Affairs publishes overarching qualitative and quantitative IT benchmark studies, including on e-security.

In 2003, the **Spanish** Association for Electronic and Communication Enterprises[452] completed an initial study to assess the overall demand for information security and communication technologies in Spain. The study provided an overview of state-of-the-art information security in Spanish industries and

---

confidential information over the Web, regularly backup crucial data files, other security countermeasures); Why use or not use it-security products (IT-security products being used, reasons for not using IT-security products, software too hard to use and/or understand, installation is difficult); Guidance about it-security products when purchasing computer or related products (how to deal with suspicious e-mails, securing against unwanted use of computer, making backup, installation of anti-virus products, clean up after virus attack).

451. Cf. Assessment of Information Security Management (VAHTI 3/2003) and the Risk Assessment Instruction to Promote Government Information Security (VAHTI 7/2003).

452. ASIMELEC - www.asimelec.es

organisations, and emphasised the insufficient level of commitment to information security in Spain, and the lack of awareness of risks and vulnerabilities.[453]

Furthermore, Red.es, an agency of the Ministry of Industry, Tourism and Commerce, has established Spain's "Telecommunications and Information Society Observatory". This body acts as a reference centre for monitoring the country's ICT developments, and is a forum for exchanging of ICT experiences between the private and public sectors. The observatory, moreover, has developed indicators to measure the overall development of the information society in Spain.[454]

In **Sweden**, the Swedish IT Incident Centre collects CSIRT relevant statistics. They have recently undertaken a study with the police on the degree of un-reported computer incidents. The Swedish Emergency Management Agency (SEMA) is collecting information and statistics from relevant actors in the society, including intelligence and security agencies, and private organisations, in order to create an overall picture of the information assurance situation. The overall picture constitutes the knowledge base for risk assessments conducted by SEMA.

In the **United Kingdom**, adherence to the ISO 17799 standard and third party assessment against the national British standard BS 7799 part 2 are two main benchmarks in use. Other sectoral and cross-sectoral benchmarking tools are being developed. The National Infrastructure Security Co-ordination Centre (NISCC) discuss with critical national infrastructure (CNI) management the resilience of their systems on the basis of a generic security model.

In the **United States**, the Computer Security Institute/ Federal Bureau of Investigation (FBI) survey of cyber-security is an important metric and benchmark for assessing the information security state of the private and public sector. Moreover, the Department of Homeland Security and the Department of Justice plan to survey 36 000 US businesses concerning the type and frequency of computer security incidents in 2005. The goal of this survey is to improve data on cybercrime to assist policy analysis for government and the private sector, and provide statistically relevant national data on cybercrime across all US businesses, especially those in critical infrastructure sectors.

Australia, the **Czech Republic, France, Norway, Portugal**, and the **Slovak Republic** do not seem to have put forward metrics and measures. Australia notes that the government is aware of the need to quantify the success of its initiatives. France indicated that there were no public indicators in France to assess the impact of the IT security measures.

453. On the contrary, anti virus products (100%) and firewalls (80%) are widely used, *cf.* (www.asimelec.es/pdf/seguridad/asimelec%20estudio%20mercado%20ISO17799-021024.pdf)

454. Recent studies of the Observatory include: Fourth campaign of TIC in Spanish homes (*Cuarta oleada las TIC en los hogares españoles*), Spanish microsociety in 2004 Information Society (*La Microempresa española en la Sociedad de la Información* 2004), Home Internet use (*Usos de Internet en los hogares*), and an Electronic Commercee study (Estudio sobre Comercio Electrónico B2C 2004).

ANNEX 2
OECD QUESTIONNAIRE ON PRACTICAL INITIATIVES TO PROMOTE A CULTURE OF SECURITY

AS CALLED FOR IN THE OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: TOWARDS A CULTURE OF SECURITY

Section I: Government as developer of public policy, law, and regulation[455]

A. Comprehensive statement of strategy

Has your country developed a national policy and/or strategy on the security of information systems and networks and the promotion of a culture of security? Is such a strategy currently being developed or are there any plans for doing this in the future?

If yes, please:

- Describe the process used to develop the strategy, including:
  - Assignment of responsibility for developing the policy.
  - Assignment for following up on the policy.
  - Involvement of relevant participants from government, the private sector and civil society in the development of the policy.
- Describe nature and scope of the strategy, including:
  - Objectives.
  - Definitions of significant terms.
  - Applicability to public/private sectors.
  - Action items covered and priorities for their implementation.
  - Timeframe and assignment of responsibilities for implementation.
  - Assessment/reassessment of the impact of the policy.
  - Consistency with the *Security Guidelines* and/or other international or regional policy instruments.
  - How the national policy is communicated to all participants.
- Describe the involvement and roles in policy development and implementation by the private sector, users and others.
- Provide Web citations.
- Provide English and/or French translations of policy documents as available and indicate whether you would like them to be published on the OECD culture of security Web site (www.oecd.org/sti/cultureofsecurity).

455. Questions 1-3 are primarily related to the policy-oriented principles (1-5) of the 2002 *OECD Security Guidelines.*

B. Legal, regulatory, and institutional arrangements to oversee and implement a culture of security

What legal, regulatory and institutional[456] arrangements has your country made to implement a culture of security? Are such arrangements currently being made or are there any plans for doing this in the future?

Please address the nine areas identified in the list below and cover the following, as far as possible:

- Describe and provide detail on the arrangements and implementation, including division of responsibilities, among various government bodies.
- Address international co-operation and information sharing, and provide points of contact for international co-operation and information sharing for items (a), (b) and (c) below.
- Describe how your country incorporates existing and developing international best practices.
- Provide Web citations.

Nine areas to address with regard to legal, regulatory and institutional arrangements

a) Cybercrime, including:
   - Substantive and procedural legislation (including pending legislation).
   - Enforcement.
   - Other (*e.g.* prevention).

b) Computer incident watch and warning, and response.

c) Critical infrastructure.

d) Risk assessment.

e) Outreach to business, civil society and others.

f) Outreach to state and local government.

g) Education and training.

h) Science and technology (S&T) and research and development (R&D).

i) International outreach and co-operation.

C. Recommendations and other voluntary efforts

Has your country developed voluntary, publicly available recommendations to assist government, business and/or users to address the security of information systems and networks? Are such recommendations currently being developed or are there any plans for doing this in the future?

If yes, please identify significant examples and provide information including:

- The nature of the recommendations.
- How they were developed.
- The involvement of the private sector and others.
- How they are disseminated.

456. For example, creating a specific body in the public administration to co-ordinate information security activities.

Section II: Government as owner and operator of systems and networks

What action has your government taken to develop a culture of security within the government itself? Is there any distinct government plan for this? What measures have been taken in each of the possible areas of government action related to its role as owner and operator of systems and networks to develop a culture of security identified in the list below? Are such measures currently being developed or are there any plans for doing this in the future? [457]

- Provide information on:
  - The assignment of responsibility for implementation.
  - Institutional arrangements (*e.g.* creating a specific body in the public administration to co-ordinate information security activities).
  - Specific initiatives taken or to be taken.
  - Creation or support of measures for self assessment (*e.g.* checklists for evaluating the security of existing systems).
- Provide details on implementation, including:
  - Priorities for implementation.
  - Progress to date on implementation and actions taken.
- Include Web citations.

Possible areas of government action related to its role as owner and operator of systems and networks

a) To secure government systems, including co-ordination among agencies/ministries.

b) To provide watch and warning and incident response for government systems. Please also address:

- The creation of or participation in computer security incident reporting team (CSIRT) or CSIRT-like institutions.
- Efforts to co-ordinate among government agencies on watch and warning and incident response (including information about criteria for and co-ordination on issuing alerts).
- Co-ordination with other stakeholders in regard to vulnerability discovery, disclosure and patch management.

c) To co-operate and co-ordinate with non-government owners and operators in your country.

d) To monitor and evaluate security compliance and effectiveness of agency owners and operators,[458] the use of risk assessments and/or audits (whether voluntary or mandatory); the methodology used, entity in charge of the audit, time periods for re-auditing, assignment of budget for auditing activities, etc.; the use of security standards in procurement; and the use of penetration tests.

Do you collect information and/or statistics on the budget for security of information systems and networks in the public sector? Do you set targets for the proportion of information security spending in the public sector in your country? If not, do you plan such or similar measures for the future?[459]

457. Question 4 is primarily related to the operation-oriented principles (6-9) of the 2002 *OECD Security Guidelines.*

458. "Agency owners and operators" refers to any government entity that would own and operate information systems and networks, such as government ministries, agencies, departments, etc.

459. This question is primarily related to the policy-oriented principles (1-5) of the 2002 *OECD Security Guidelines.*

Section III: Government as user of information systems[460]

What have been the most effective programmes and initiatives taken by your government in its efforts to develop a culture of security among users of government systems? Are such programmes/initiatives currently being developed or are there any plans for doing this in the future?

Please:

- Describe the programme(s) and initiative(s).
- Provide details on implementation.
- Include Web citations.

Section IV: Government as partner with business and industry[461]

What were the most successful government collaborative initiatives with, and outreach to, small and medium-sized enterprises (SMEs) to promote a culture of security? Are such initiatives currently being developed or are there any plans for doing this in the future?

- Describe the initiatives.
- Provide details on implementation.
- Include Web citations.

What are the most successful initiatives and approaches used by your government for outreach to business and industry to foster a culture of security among business and industry and develop public-private co-operation in each of the following areas. Please also describe initiatives and approaches planned for the future.

- Describe the initiatives/approaches.
- Provide details on implementation, including the division of responsibility between government and the private sector.
- Include Web citations.

Areas to consider with regard to successful approaches to foster a culture of security among business and industry and develop public-private co-operation

a) Awareness-raising.
b) Education and training, including distance learning.
c) Watch and warning and emergency response.
d) Corporate Governance and ethics.
e) Creation and implementation of corporate security policies.
f) Prevention and combating of cybercrime.
g) Development of secure software.
h) Technical (including management) standards.
i) Independent certification of the security of information technology.
j) Other relevant areas.

460. Question 6 is primarily related to the operation-oriented principles (6-9) of the 2002 *OECD Security Guidelines.*

461. This section is meant to address both the policy-oriented principles (1-5) and the operation-oriented principles (6-9) of the 2002 *OECD Security Guidelines.*

Section V: Government as partner with civil society[462]

What were the most successful government collaborative initiatives with, and outreach initiatives to, civil society to promote a culture of security for information systems and networks among users (including households and the general public)? Are such initiatives currently being developed or are there any plans for doing this in the future?

Please:

- Describe the initiative(s) and its/their implementation.
- Discuss division of responsibility between government, civil society and the private sector (businesses).
- Provide Web citations.

What were the most successful government initiatives in the education system in your country (pre-school age, all school ages, and higher education) to address the culture of security? Are such initiatives currently being developed or are there any plans for doing this in the future?

Please:

- Describe the initiative(s).
- Provide details on implementation.
- Include Web citations.

Section VI: Government efforts related to S&T and R&D

What Science and Technology (S&T) and Research and Development (R&D) activities does your government have underway (or planned) related to a culture of security in each of the following areas?

Please:

- Describe the scope, timeframe and size of such initiatives (budgets in EUR).
- Provide details on implementation.
- Discuss the involvement of the private sector and/or academia.
- Include Web citations.

Possible areas in which government may have S&T and R&D activities

a) Vulnerabilities.

b) Best practices.

c) Security standards.

d) Development of secure software (*e.g.* methodologies).

e) Benchmarks and metrics for measuring the security of information systems and networks and the impact of respective initiatives.

f) Other.

462. This section is meant to address both the policy-oriented principles (1-5) and the operation-oriented principles (6-9) of the 2002 *OECD Security Guidelines.*

Section VII: Metrics and benchmarks

Have metrics and/or benchmarks for measuring the impact and/or success of your government's activities for Sections I-VI above been developed in your country? Are there any plans for doing this?[463]

If yes, please:

- Identify indicators being used/considered.
- Describe how measures are being implemented (including the foreseen frequency of measuring).
- Describe the results of measurements undertaken.
- Provide Web citations as available.

463. Related principles of the OECD *2002 Security Guidelines* for this question are: Security management, Reassessment.