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

02-Jul-2003

English - Or. English

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

DSTI/ICCP/REG(2003)5/REV1
Unclassified

Working Party on Information Security and Privacy

IMPLEMENTATION PLAN FOR THE OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: TOWARDS A CULTURE OF SECURITY

This Implementation Plan has been revised to include comments received from delegates. This document will be issued to the ICCP on 2-3 October. It will be issued to participants at the Oslo Workshop on Information Security on 13-14 October. It will be further revised following the discussions at the Oslo Workshop, if necessary.

Contact: Anne Carblanc, Tel: +33 1 45 24 93 34; anne.carblanc@oecd.org;
Fax: +33 1 44 30 62 59; www.oecd.org/sti/security-privacy

JT00147018

English - Or. English

IMPLEMENTATION PLAN FOR THE OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: *TOWARDS A CULTURE OF SECURITY*

I. Promoting a global "Culture of Security"

1. The revised *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (the "Guidelines") that were adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002, represent a significant step forward in the OECD's efforts to promote a "Culture of Security" among all participants who develop, own, provide, manage, service and use information systems and networks, whether those participants are from government, business or civil society. These guidelines have been the basis for considerable implementation efforts at the national level, and are the basis for Resolution A/RES/57/239 adopted by the 57th session of the United Nations General Assembly.

2. The Guidelines respond to the ever-changing nature of the security environment by promoting the development of a culture of security – that is, a focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving by all participants when using information systems and communicating or transacting across networks. The Guidelines signal a clear break with a time when secure design and use of networks and systems were too often afterthoughts. Participants are becoming more dependent on information systems, networks and related services, all of which need to be reliable and secure. Only an approach that recognises the interests of all participants, and the nature of the systems, networks, data and related services, can provide effective security. An effective action programme, well planned and co-ordinated is now essential for the implementation of the Guidelines and the promotion of a culture of security.

3. These voluntary Guidelines constitute a foundation for work towards a culture of security. The principles of Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment apply to all participants, but differently, depending on their roles in relation to information systems and networks. Leadership in pursuit of policies that will support the aims and objectives of these principles is essential and should encourage all participants to adopt and promote a culture of security as a way of thinking about, assessing, and acting on, the operations of information systems and networks. The promotion of a culture of security will require not only leadership but also broad participation at all levels of government, business, and civil society to heighten the priority for security planning and management, as well as to increase understanding of the need for security among all participants. The Guidelines and the related outreach campaigns should encourage participants to factor security into the design, implementation, and use of all information systems and networks.

4. Each participant is an important actor in the process of ensuring security. Participants, as appropriate to their roles, should be aware of the relevant security risks and preventive measures, assume responsibility and take steps to enhance the security of information systems and networks. They should recognize that the principles are complementary and meant to be read as a whole. Involvement of the private sector, which designs, builds, owns and operates most of the infrastructure of information systems

and networks, is required for the promotion of a culture of security. Business as well as other participants is also encouraged to formulate their own initiatives to implement the Guidelines.

5. Continued co-operation among government, business and civil society is also required in follow-up work on the Guidelines. Public-private partnerships offer a good platform for fostering such relationships. Government, as well as industry and civil society, should address the Awareness Principle first, as participants' awareness of risks to information systems and networks, as well as what they can do to address those risks, is fundamental. Without awareness, action to implement the other principles is unlikely. Likewise, embracing the Responsibility Principle is a matter of urgency and will require a new and imaginative partnership among member and non-member countries, government entities, and other participants.

II. Roles of government

6. Government has a responsibility to provide leadership in developing a culture of security. It should provide this leadership in each of its roles related to information systems and networks that include the development of public policy, as owner and operator of systems and networks, and as a user of such systems and networks. In developing public policy, government should promote the security of information systems and networks to engender confidence in their use and better ensure economic growth and overall security. Public policy development is a unique role of government but one that should be carried out in a transparent fashion and in consultation with other participants and concerned parties. Of particular note in this regard is government's responsibility for *(a)* awareness-raising; *(b)* ensuring the provision of education and training; and *(c)* the provision of information resources to the public, an activity that also assists government in fulfilling its other roles. As owner and operator of information systems and networks, government shares a role with businesses and other organisations and has responsibilities to lead by example. As a user of information systems and networks government shares a role with businesses, other organisations, and individuals for ensuring use of the system and network consistent with a culture of security. The following sections look more closely at government's responsibilities and opportunities in these various roles.

A. *Government responsibility for public policy*

1. Develop national policy on information security and ensure cross-border co-operation to promote a global culture of security.

7. Government should recognize the increasing need for a comprehensive policy and institutional infrastructure to ensure public safety, security and economic well-being in response to the threats and vulnerabilities associated with globally interconnected information systems and networks. Governments are further encouraged to respond by establishing new or amend existing policy that may incorporate principles of the Guidelines. In doing so, principles in the Guidelines may need to be aligned with the national situation in the area, and ongoing or planned national initiatives. Such initiatives may include policies to combat cyber crimes, such as:

- Enacting a comprehensive set of substantive criminal, procedural and mutual assistance legal measures to combat cybercrime and ensure cross-borders co-operation. These should be at least as comprehensive as, and consistent with, the Council of Europe Convention on Cybercrime (2001).
- Identifying national cybercrime units and international high-technology assistance points of contact and creating such capabilities to the extent they do not already exist; and
- Establishing institutions that exchange threat and vulnerability assessments [such as national CERTs (Computer Emergency Response Teams)].

- Developing closer co-operation between government and business in the fields of information security and fighting cybercrime.

8. The development of these policies should be consistent with the Guidelines, in particular, the principles on ethics and democracy that provide the societal references for addressing security. These public policies should also be developed in conjunction with other participants (business, other organisations and users) to better ensure transparency and that the aims of the Guidelines' principles can be met in an effective manner.

2. Outreach and support for other participants

9. A second aspect of government's public policy role is to conduct outreach and support efforts by all participants to address security. In the first instance government action should raise awareness of law and policy that address cybersecurity. Beyond this, government should facilitate awareness and appropriate responses by other participants through programmes and initiatives.

10. These efforts could include, but not be limited to, highlighting the nature of the problem, assisting participants to address their security responsibilities, supporting education and training, establishing points of contact and resource sites for practical information, and removing obstacles to action by participants. Government should also consider support for R&D, the development of best practices, and building partnerships among participants to address information security. As part of its public policy role, government can utilise its significant purchasing power and system/network size to support efforts to increase security through improved security in software, hardware, and best practices operational procedures. This public policy role also extends to addressing response to and recovery from cyber incidents.

11. Awareness raising can be achieved through consistently emphasising the necessity of security at every opportunity. Education, training, press releases, Web sites, public announcements, offering tools and kits are among the current identified means to raise awareness. Government should continue to emphasise the importance of awareness of the risks and available safeguards to participants. Such awareness-raising campaigns should aim to ensure that participants become fully aware that:

- Information systems and networks can be affected by both internal and external risks.
- Security failures may significantly harm systems and networks both under and outside of their control.
- There is potential harm to and from others arising from interconnectivity and interdependency.
- It is important to understand the configuration of, and the availability of updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.
- They should adopt safeguards/solutions to deal with known threats and vulnerabilities.
- They should develop security goals that are appropriate to their needs in preventing, detecting and responding to threats and vulnerabilities.
- They should be accountable in a manner appropriate to their individual roles.
- They should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environments.

12. Examples of initiatives in this category can be found on the Web sites of several governments including at the US Federal Trade Commission:

http://www.ftc.gov/bcp/conline/edcams/infosecurity/forkids.html

13. Exchange of best practice should facilitate users' ability to better understand and achieve the goal of effective and up-to-date security measures.

14. In designing education and information programmes, not only tips to ensure the security of the systems and networks are necessary, but also emphasis on the ethics to promote conduct that recognizes security needs and respects the legitimate interests of others. Government initiated education and outreach programmes should also promote conduct that aims at ensuring security in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency. Assessing the impact of planned security measures on these values should also be encouraged.

15. Further efforts are necessary so that users of the systems and networks should know how to set up and maintain their systems and networks, be aware of the latest vulnerabilities, and know whether or not software patches are available. They should also know what to do when security incidents occur, including timely action for seeking help.

16. Further efforts are necessary for the development of information security educational programmes wherever IT use is taught, such as in engineer education, health education or general computer education programmes currently undertaken in schools and universities.

17. Useful sites such as those of CERT[1] or SANS[2] and various industry information sharing and analysis centres (ISAC) have been established. Further efforts are necessary to continue to support such initiatives to establish sources of practical information and publication of the references to such sources. Governments should encourage participants, especially business, to utilise, share and distribute useful information through such institutions.

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

18. Government must address the principles of risk assessment, security design and implementation, security management, and reassessment, just as any other owner and operator of information systems and networks. Government should develop policies that reflect best practices in security management and risk assessment. Security management should be based on a risk assessment that identifies threats and vulnerabilities and is sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Government's security management should also be dynamic, encompassing all levels of government's activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. And, these information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. Internationally recognised information security management standards, such as ISO standards and industry-specific standards, may be used to establish an effective system of security management.

19. Because of the size of its operations, government has a special responsibility to become a model owner/operator and to lead by example. Government can thus use its operational expertise to facilitate the development of best practices and other operational improvements for the benefit of all participants.

1. Computer Emergency Response Team, Carnegie-Mellon University: http://www.cert.org/.

2. SANS (SysAdmin, Audit, Network, Security) Institute. For example, in October 2002, SANS Institute and the FBI released a list summarising the Twenty Most Critical Internet Security Vulnerabilities; http://www.sans.org/top20/.

Government can also use its significant purchasing power in information systems and networks to encourage the development and expanded availability of more secure products and services.

C. Government as user of information systems and networks

20. As a user of information systems and networks, government has a responsibility to ensure that its use is consistent with the Guidelines, in particular the ethics and democracy principles, and thus contributes to a secure global system. Because individual government employees constitute government use, government must ensure its employees are aware of security concerns, their individual responsibilities and have the capability to respond in an appropriate way to security incidents. Development by government of an appropriate security environment, training, and tools will not only facilitate security on government systems and networks, but can also serve as foundation elements for government's outreach as a public policy matter.

III. Roles of business and civil society

A. Business as owner and operator of information systems and networks

21. As with government, business must address the principles of risk assessment, security design and implementation, security management, and reassessment. Security management should be based on a risk assessment that identifies threats and vulnerabilities and is sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. This will be enhanced through ongoing dialogue between business and government.

22. The ICT industry in particular has a role in ensuring that their products and services reflect sound security practices. In this regard the industry can play a leadership role in the development of internationally accepted standards, including through, but not limited to, involvement in the activities of standards bodies such as ISO[3] and IETF.[4]

B. Business and civil society as users of information systems and networks

23. As users of information systems and networks, business and civil society have a responsibility to ensure that their use is consistent with the Guidelines, in particular with the security design and implementation and security management principles, and thus contributes to a secure global system. This will be facilitated in part by government's awareness-raising activities referred to under II.A.2, but also must be a matter of initiative taken on by each participant.

3. The International Organisation for Standardisation.

4. The Internet Engineering Task Force.