ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Directorate for Science, Technology and Industry
Committee for Information, Computer and Communications Policy

OECD Recommendation of the Council on the Protection of Critical Information Infrastructures

[C(2008)35]

OECD Ministerial Meeting
on the Future of the Internet Economy

Seoul, Korea, 17-18 June 2008

Hosted by 방송통신위원회
KOREA COMMUNICATIONS COMMISSION

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

Foreword

This Recommendation was developed by the OECD Committee for Information, Computer and Communication Policy (ICCP Committee), and its Working Party on Information Security and Privacy. The Recommendation was adopted by the OECD Council at its 1172nd Session on 30 April 2008.

OECD Recommendation of the Council on the Protection of Critical Information Infrastructures

THE COUNCIL

Having regard to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

Having regard to the Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security [C(2002)131], hereinafter the "Security Guidelines";

Having regard to the Resolution 58/199 adopted by the General Assembly of the United Nations on the creation of a global culture of cybersecurity and the protection of critical information infrastructures;

Recognising that the functioning of our economies and societies increasingly relies on information systems and networks that are interconnected and interdependent, domestically and across borders; that a number of those systems and networks are of national critical importance; and that their protection is a priority area for national policy and international cooperation;

Recognising that in order to improve the protection of domestic and cross-border critical information infrastructures, Member countries need to share their knowledge and experience in developing policies and practices and cooperate more closely between themselves as well as with non Member economies;

Recognising that the protection of critical information infrastructures requires coordination domestically and across borders with the private sector owners and operators of such infrastructures, hereinafter the “private sector”;

On the proposal of the Committee for Information, Computer and Communication Policy:

AGREES that:

For the purposes of this Recommendation, critical information infrastructures, hereinafter “CII”, should be understood as referring to those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy;

National CII are identified through a risk assessment process and typically include one or more of the following:

- Information components supporting critical infrastructures, and/or

- Information infrastructures supporting essential components of government business; and/or
- Information infrastructures essential to the national economy.

RECOMMENDS that:

Member countries introduce and maintain an effective framework to implement the OECD Security Guidelines in relation to the protection of CII, taking into account the specific policy and operational guidance set out herein;

PART I. Protection of critical information infrastructures at the domestic level

Member countries should:

Demonstrate government leadership and commitment to protect CII by:

- Adopting clear policy objectives at the highest level of government.
- Identifying government agencies and organisations with responsibility and authority to implement these policy objectives.
- Consulting with private sector owners and operators of CII to establish mutual cooperation for the implementation of these objectives.
- Ensuring transparency on the delegations of responsibility to government authorities and agencies to facilitate closer co-operation within the government and with the private sector.
- Systematically reviewing policy and legal frameworks and self-regulatory schemes which may apply to CII, including those addressing cross-border threats, to assess the need to enhance their implementation, to amend them or to develop new instruments.
- Taking steps, where appropriate, to enhance the security level of components of information system and networks that constitute CII.

Manage risks to CII by:

- Developing a national strategy that gains commitment from all those concerned, including the highest levels of government and the private sector.
- Taking into consideration interdependencies.
- Conducting a risk assessment based on the analysis of vulnerabilities and the threats to the CII, in order to protect economies and societies against the impacts of highest national concern.
- Developing, on the basis of the assessment, and periodically reviewing a national risk management process that sets out the detailed organisation, tools and monitoring mechanisms required to implement the risk management strategy at every level, including:
    - *i.* The appropriate organisational structure to provide guidelines and promote good security practices at the national level and to manage and monitor progress, as well as a complete set of processes to ensure

preparedness, including prevention, protection, response and recovery from natural and malicious threats.

ii. A system of measurement to evaluate and appraise measures in place (including exercises and tests as appropriate) and allow for feedback and continuous update.

- Developing an incident response capability, such as a computer security incident response team (CERT/CSIRTs), in charge of monitoring, warning, alerting and carrying out recovery measures for CII; and mechanisms to foster closer cooperation and communications among those involved in incident response.

Work in partnership with the private sector by:

- Establishing trusted public-private partnerships with a focus on risk management, incident response and recovery.
- Enabling mutual and regular exchange of information by establishing information sharing arrangements that acknowledge the sensitivity of certain information.
- Fostering innovation through public-private research and development projects focused on the improvement of the security of CII and as appropriate, sharing these innovations across borders.

PART II. Protecting critical information infrastructures across borders

Member countries should cooperate among themselves and with the private sector at the strategy, policy and operational levels to ensure the protection of CII against events and circumstances beyond the capacity of individual countries to address alone.

They should in particular proactively engage in bilateral and multilateral cooperation at regional and global levels with a view to:

- Share knowledge and experience with respect to the development of domestic policies and practices and to models for coordinating with private sector owners and operators of critical information infrastructures.
- Develop a common understanding of:

  i. Risk management applicable to cross-border dependencies and inter-dependencies.

  ii. Generic vulnerabilities, threats and impacts on the CII, to facilitate collective action to address those that are widespread, such as security flaws and malicious software, as well as to improve risk management strategies and policies.

- Make available information regarding the national agencies involved in the protection of CII, their roles and responsibilities, to facilitate identification of counterparts and improve the timeliness of cross border action.
- Acknowledge the value of participation in international or regional networks for watch, warning and incident response, to enable robust information

sharing and coordination at the operational level, as well as to better manage crisis in case of an incident developing across borders.

- Support cross-border collaboration for, and information sharing on, public-private research and development for the protection of CII.

INVITES:

Member countries to disseminate this Recommendation throughout the public and private sectors, including governments, businesses and other international organisations to encourage all relevant participants to take the necessary steps for the protection of CII;

Non-Member economies to take account of this Recommendation and collaborate with Member countries in its implementation;

INSTRUCTS the OECD Committee for Information, Computer and Communication Policy to:

Promote the implementation of this Recommendation and review it every five years to foster international co-operation on issues relating to the protection of CII.