G8 Principles for Protecting Critical Information Infrastructures

(Adopted by the G8 Justice & Interior Ministers, May 2003)

Information infrastructures form an essential part of critical infrastructures. In order effectively to protect critical infrastructures, therefore, countries must protect critical information infrastructures from damage and secure them against attack. Effective critical infrastructure protection includes identifying threats to and reducing the vulnerability of such infrastructures to damage or attack, minimizing damage and recovery time in the event that damage or attack occurs, and identifying the cause of damage or the source of attack for analysis by experts and/or investigation by law enforcement. Effective protection also requires communication, coordination, and cooperation nationally and internationally among all stakeholders – industry, academia, the private sector, and government entities, including infrastructure protection and law enforcement agencies. Such efforts should be undertaken with due regard for the security of information and applicable law concerning mutual legal assistance and privacy protection. To further these goals, we adopt the following PRINCIPLES and encourage countries to consider them in developing a strategy for reducing risks to critical information infrastructures:

I. Countries should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.

II. Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.

III. Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.

IV. Countries should promote partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.

V. Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.

VI. Countries should ensure that data availability policies take into account the need to protect critical information infrastructures.

VII. Countries should facilitate tracing attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other countries.

VIII. Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities.

IX. Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries as appropriate.

X. Countries should engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analyzing information regarding vulnerabilities, threats, and incidents, and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.

XI. Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.