Critical Information Infrastructure Protection: Communiqué

Protecting our critical infrastructures from terrorist and criminal attack and responding to such activity is a topic of great importance to the vitality of our economies and the safety and security of our citizens. Since the first G8 meeting on this in 1997, we have encouraged greater cooperation and coordination among law enforcement and other partners in government and the private sector.

In 2003, we adopted the "G8 Principles For Protecting Critical Information Infrastructures." One of these Principles states that countries should conduct exercises to enhance their response capabilities. In May 2005, the G8 High-Tech Crime experts hosted the successful "Unified Response" Tabletop Exercise in New Orleans, where experts in law enforcement, watch and warning, and industry met to find solutions to challenges we face in protecting our critical information infrastructures. This exercise enhanced prevention, cooperation, communication, and response among law-enforcement, watch and warning organizations, and the private sector in G8 countries for attacks on critical information infrastructures, and provided a basis to advance our strategy among these entities, both within and outside the G8. We are pleased with the results of this unique gathering and agree in the coming year to take further action in the following five areas:

- We must continue to enhance communication and information-sharing between watch and warning organizations and law enforcement both domestically and internationally, including better reporting of possible criminal activity;

- We must ensure that all G8 countries have, and encourage other countries to develop, watch and warning organizations able to detect vulnerabilities and threats; prevent these threats from causing harm, and disseminate relevant information to any threatened region or country in a quick and efficient manner;

- We must ensure that our law enforcement agencies can quickly respond to serious cyber threats and incidents; therefore, we must work towards providing access to data necessary for attribution of illegal conduct, regardless of where the specific terrorist or criminal activity originates or the victim is located;

- We must continue and strengthen our work with the private sector to identify vulnerabilities and threats, increase reporting of cyber incidents and improve the response capabilities of law enforcement, watch and warning communities, and industry; and

- We must continue to conduct national and multinational training and exercises in order to further improve readiness and strengthen global communication, coordination, and response concerning attacks on our critical infrastructures.