

The G8 24/7 Network for Data Preservation Protocol Statement

HOW THE G8 24/7 NETWORK OPERATES

The G8 24/7 points of contact are provided for investigations involving electronic evidence that require urgent assistance from foreign law enforcement. High-tech crimes raise new challenges for law enforcement. In investigations involving computer networks, it is often important for technically literate investigators to move at unprecedented speeds to preserve electronic data and locate suspects, often by asking Internet Service Providers to assist by preserving data. Therefore, to enhance and supplement (but not replace) traditional methods of obtaining assistance, the G8 has created the Network as a new mechanism to expedite contacts between Participating States or other autonomous law enforcement jurisdictions of a State (hereinafter referred to as "Participants").

To use this network, law enforcement agents seeking assistance from a foreign Participant may contact the 24-hour point of contact in *their own* state or autonomous law enforcement jurisdiction, and this individual or entity will, if appropriate, contact his or her counterpart in the foreign Participant. Participants in the Network have committed to make their best efforts to ensure that Internet Service Providers freeze the information sought by a requesting Participant as quickly as possible. Participants have further committed to make their best efforts to produce information expeditiously. This is subject to the understanding that a requested Participant's legal, technical or resource considerations may affect the extent to which – and the time frame within which – the Participant may produce evidence, as well as the process of Mutual Legal Assistance, by which the requesting country seeks release of that information through the usual MLAT or Letters of Request procedure.

To date, the number of requests made has been small – this is particularly true for requests outside of business hours – but members find the contacts list useful in many ways. For example, in relation to a \$10 million bank robbery when a Norwegian police officer was shot dead. Norwegian Police used the Network to request the UK to preserve computer data, which led to the suspect (Norway's most wanted criminal) being located within days at an internet cafe in Spain, where he was arrested by Spanish police.

MEMBERS OF THE G8 24/7 NETWORK (as of February 2007)

Australia	Germany	Malaysia	Philippines
Austria	Hong Kong, China	Malta	Romania
Brazil	Hungary	Mauritius	Russia
Bulgaria	India	Mexico	Singapore
Canada	Indonesia	Morocco	South Africa
Chile	Israel	Namibia	Spain
Croatia	Italy	Netherlands	Sweden
Czech Republic	Jamaica	New Zealand	Taiwan
Denmark	Japan	Nigeria	Thailand
Dominican Republic	Republic Of Korea	Norway	Tunisia
Finland	Lithuania	Pakistan	United Kingdom
France	Luxembourg	Peru	United States

MEMBERSHIP CRITERIA

To join the Network, an applicant must be able to provide the following four things:

- **Contact point available 24/7**

This means a person who can be reached 24 hours a day, 7 days a week, to receive information and/or requests for assistance from other countries within the Network. Becoming a contact point does *not* require the establishment of a formal computer crime unit. In some jurisdictions, the contact point consists of a few investigators interested in cybercrime; in others, the contact point is part of a formal unit.

In addition, some contact points are telecommunication centers that connect the caller to an appropriate official, while others are personnel with investigative and/or technical expertise. For example, one way to implement a contact point is to have four or five staff who are high-tech crime investigators on a rota system where each person is reachable outside normal working hours by a mobile phone which he or she keeps for one week out of every month.

- **English speaking contact point**

This is for reasons of practicality because the network is far simpler if there is a common language, and English is the most widely spoken language, particularly in relation to computing and the Internet.

- **Technically knowledgeable contact point**

The person to whom calls are referred to should have a basic level of knowledge of computer crime, for example being able to understand what a “distributed denial of service” attack is, what the caller means when he or she asks for IP logs to be preserved, etc. Such knowledge can be gained in a basic computer crime course.

- **Knowledgeable about domestic laws and policies**

As a law enforcement cybercrime investigator, the person responding to the request should have an understanding of his or her authority to preserve or collect electronic evidence. In addition, he or she should know, or have the ability to quickly find out, what types of assistance to foreign countries are permitted by domestic laws.

FURTHER INFORMATION

The directory of countries that are members of the G8 24/7 Network is compiled and maintained by the G8 Subgroup on High-Tech Crime. A sample entry is shown below, together with a list of the forty countries that are currently members. Members of the network should not publicly disclose the list or post it on a website. The point of contact should, however, make it clear to domestic law enforcement authorities that the point of contact exists and is available to handle international requests for assistance.

If you have questions or comments about membership, please contact the Subgroup chair, Christopher Painter (christopher.painter@usdoj.gov) in the United States at +1.202.514.1026. Alternatively, you may wish to discuss joining the Network with a representative on the high tech crime subgroup from any of the G8 Countries (Canada, France, Germany, Italy, Japan, Russia, United Kingdom and United States). If accepted, your contact details will be added to the directory, which is circulated by email to all member countries. Training is provided periodically to help contact points undertake their duties, and tests of the Network are made to ensure contact points are continuing to meet the criteria for membership.

Sample Entry for Member State Contact Information

Contact & Telephone Number:

High Tech Crime Coordination Team
Any Police Department
100 Main Street
City A, State or Province B
Sample Jurisdiction

Tel: 1-1-1111-1111 or 1-1-1111-1112
Fax: 1-1-1111-1113
E-mail: htct@police.gov.sj

Description of Contact:

The High Tech Crime Coordination Team (HTCCT) is the 24/7 central point of contact for all of Sample Jurisdiction's international and Interpol NCB commitments. The HTCCT is also the contact point responsible for investigating computer intrusions, viruses, and denial-of-service attacks as well as other crimes enabled by computer. Sample Jurisdiction maintains electronic evidence recovery capabilities in its two major cities (City A and City B) to support criminal investigations if evidence preservation and recovery is required.

Language Capabilities of Contact:

English and French only.

What to Say When Calling Contact Number:

Please state that this is a G8 high-tech emergency, the nature of the emergency including specific details with respect to the source of the activity, the victim and related technical information, the assistance requested and your contact details. If sending details electronically, please use the Interpol Computer Crime Message format. Please also include detailed time-zone information including GMT/UTC offsets (e.g. "GMT +6 to allow conversion to Sample Jurisdiction's local time-zones).

In case of a difficulty that cannot be resolved, please contact:

Director Marc Faratine
Sample Jurisdiction High Tech Crime Centre
Tel: 11-1-1111-1011
Fax: 11-1-1111-1012

Time Zone: UTC/GMT +6:00 hours