Group of Eight (G8)
High-Tech Crime Subgroup

Challenges Associated with Emerging Technologies For Law Enforcement
Wireless Local Area Networks (WLANs)

WIRELESS LOCAL AREA NETWORK (WLAN) BEST PRACTICES FOR LAW ENFORCEMENT

- Encourage training relating to wireless networking technologies for law enforcement investigators and prosecutors involved in the investigation or prosecution of criminal offenses involving WLAN devices or technologies.

- Ensure that law enforcement officers and prosecutors are aware of specific legislation that criminalizes the intrusion, interception, attack, unauthorized use of WLANs.

- Consider the use of lawful network monitoring technologies to detect security incidents, identify the source of criminal activity, and to protect against future security incidents.

- Ensure that the existence of wireless networks and devices are taken into consideration when obtaining search warrants involving computer networks and that effective measures are taken to identify all networking components attached to the network.

- Preserve wireless access point log data (i.e. association logs and authentication logs) and network level audit, authentication, and intrusion detection system logs to identify wireless device associations, authorized network connections, and unauthorized network access attempts.

- Ensure a continued awareness of emerging security technologies and vulnerabilities affecting WLANs through the government, private sector, and educational institution initiatives related to wireless networking security and technologies.

November 2004