U. S. Department of Justice

MAR 11 1998

MEMORANDUM FOR DEPARTMENT OF JUSTICE EMPLOYEES

FROM: Stephen R. Colgate
                 Assistant Attorney General
                   for Administration

SUBJECT: Official Use of the Internet

This memorandum supplements the policy information provided in my January 13, 1997, memorandum to all Department of Justice (DOJ) employees entitled "Personal Use of the Internet" (copy attached). The following guidance is intended to clarify a few common misconceptions regarding use of the Internet when conducting DOJ official business, and to make you aware of Internet security vulnerabilities.

First, the Internet is an unregulated, global, public network comprised of interconnected networks. Today, many DOJ employees send unencrypted e-mail across the Internet. Unencrypted Internet e-mail is subject to disclosure or alteration of content and can be read by many people much like a common postcard sent through the United States mail.

The integrity and privacy of information, contained in Internet e-mail, can be achieved through the effective application of digital signature and encryption technology. The Department is working on several test projects using these technologies to test several techniques for secure information sharing. These projects are scheduled for Spring 1998. The results of these projects will provide input to the development of a Departmentwide standard and solution for e-mail and other information sharing techniques. We are working to address policy and other long-term technical issues related to the use of digital signature and encryption technology. Until strong security tools and techniques are developed and made available to DOJ employees, special care must be exercised to avoid compromising sensitive information.

Second, the speed and success of Internet e-mail transmission
depends on the availability of network resources outside the
control of either sender or receiver. Network processing
problems can cause errors and significant delays in delivery.
In some cases, messages may never be delivered. Unfortunately,
most Internet e-mail software does not provide the sender with
any method to validate the delivery or receipt of a transmitted
message. In cases where rapid delivery or proof of receipt is
important, employees must rely on other methods to confirm
receipt, such as follow-up telephone contact.

Third, employees should be aware that when they access the
Internet, using Netscape or Microsoft Explorer, they employ a
technique known as "cookies" to facilitate the gathering and
distribution of information. However, the use of "cookies"
presents several potential risks to data confidentiality,
integrity, and availability. These potential risks include:
(1) automatic collection of data without the user's knowledge
(such as credit card information or web sites and subjects
accessed), (2) transmission of the collected information to
parties unknown, and (3) the association of information about a
DOJ user's Internet activity with DOJ. Current versions of
Netscape and Microsoft Explorer browsers are set by default to
respond to "cookies" when prompted to do so, but can be
reconfigured to notify the user and permit them to refuse
requests to produce them. Technical questions regarding browser
configuration can be directed to the Internet Help Line on
(202) 305-2810.

Additionally, a file downloaded from an Internet web site may
contain computer viruses or other unwanted programs or files.
Employees must scan downloaded files for computer viruses before
attempting to open the file on any DOJ workstation. McAfee
VirusScan and Norton Antivirus are examples of acceptable
products for detecting the presence of a virus on a hard disk or
floppy disk.

Specific information regarding planned public key infrastructure
and digital signature pilot activities that support secure
Internet e-mail can be obtained from Jerry Ormaner, Assistant
Director, Information Management and Security Staff, on
(202) 514-4292.

Attachment