NR 99-18
FOR IMMEDIATE RELEASE
Contact: Dean DeBuck (202) 874-4876
March 5, 1999

OCC Issues Guidance to Protect National Banks from Intrusions Into Computer Systems

WASHINGTON, D.C. -- The Office of the Comptroller of the Currency (OCC) issued guidance to national banks today outlining the risks posed by intrusions into bank computer systems by cyber-terrorists and others. These outside threats can disrupt computer systems and corrupt or destroy information stored on computer networks.

The OCC guidance outlines risks posed by cyber-terrorist attacks: compromise of proprietary, private or classified information; destruction of computer databases and codes; and manipulation of computer, cable, satellite or telecommunications services.
Damage also can originate with employees and others with access to internal systems who can sabotage systems by causing them to crash, or by destroying, deleting or changing data.

"Although these intrusions into national bank systems are very rare, our goal is to raise awareness on this issue and ensure that national banks are taking appropriate precautions," said Clifford A. Wilke, Director of Bank Technology at the OCC. "The current growth of technology within the industry requires that national banks employ appropriate countermeasures to protect themselves against the potential threat of systems intrusions."

Today's guidance follows an OCC bulletin issued in February 1998 on technology risks that also addressed the need to protect mission-critical systems from intrusions. That bulletin was followed in August by guidance on personal computer banking that discussed the security challenges from public networks, such as the Internet. Today's bulletin continues the OCC's efforts to assist national banks as they take advantage of technology.

Technological advances and the growing interdependence of financial systems give rise to the potential for greater vulnerability to a wide range of systems intrusions, including computer viruses. The growing linkages in these systems mean that a successful attack on one network can have an impact on others.

The key to addressing the threat from systems intrusions is strong intrusion detection systems. These systems, which are readily available, identify deviations from normal communications. A strong system can resist attacks and is difficult to circumvent. A strong system can even detect the unsuccessful intrusions that often precede successful intrusions.

A good defense against systems intrusions is a combination of regular monitoring of network activity, regular reminders to employees of bank security policies and a well-configured firewall. Firewalls combine hardware and software to block unwanted communications into and out of a network.

Specific countermeasures are the use of passwords for separate electronic transactions, transmission encryption, log-in banners that warn unauthorized users of monitoring, and telephone traps and traces to isolate and identify intrusions.

National banks have been advised previously by the OCC that computer crimes must be reported to appropriate law enforcement agencies. This is particularly important in detecting coordinated systematic intrusions that can affect more than one bank.

Today's guidance may be obtained by writing to Comptroller of the Currency, Public Information Room (Mail Stop 1-5), Washington, D.C. 20219; faxing a request to (202) 874-4448; retrieving the document from the OCC Web page at http://www.occ.treas.gov; or visiting the OCC's Public Information Room at 250 E Street, S.W. in Washington, D.C. (9 a.m.-noon and 1-3:30 p.m., Monday-Friday).

# # #

The OCC charters, regulates and examines approximately 2,600 national banks and 66 federal branches and agencies of foreign banks in the United States, accounting for 58 percent of the nation's banking assets. Its mission is to ensure a safe, sound and competitive national banking system that supports the citizens, communities and economy of the United States.