NEWS RELEASE

Comptroller of the Currency
Administrator of National Banks

NR 2000-36

FOR IMMEDIATE RELEASE
May 16, 2000

Contact: Dean DeBuck
(202) 874-4876

OCC Issues Guidance on Threat of Intrusions to Bank Computer Systems

WASHINGTON -- The Office of the Comptroller of the Currency (OCC) today issued updated guidance to national banks on how to prevent, detect and respond to intrusions into their computer systems. Today's guidance supplements an OCC bulletin on cyber-terrorism published last year and an alert on distributed denial of service attacks issued in February.

As information systems become more connected and interdependent, the risk of intrusions to banks is increasing. Recent e-mail-based viruses and denial of service attacks earlier this year demonstrate increased vulnerabilities of banks that rely on the Internet. In response to these risks, banks should establish better controls and participate in information sharing organizations.

"Banks have a long history of protecting their customers' confidential information and funds," said Clifford Wilke, Director of Bank Technology. "This guidance will help national banks continue to protect their computerized information systems against intrusions by outside hackers and others. The recent e-mail based virus attacks underscore the importance of being vigilant and prepared."

Today's guidance discusses controls that can be employed to prevent and detect intrusions, ranging from basic security procedures, such as employee and contractor background checks, to technology-based tools, such as data encryption and real-time intrusion detection software. The bulletin encourages national banks to perform intrusion risk assessments, implement controls, establish intrusion response policies and procedures, and perform periodic testing.

Today's guidance also reminds national banks to report intrusions and other computer crimes to law enforcement authorities and regulators by filing Suspicious Activity Reports. The bulletin provides guidance for gathering and handling information on intrusions, and highlights three organizations that are primarily involved with the Federal government's national information security initiatives: Carnegie Mellon University's Computer Emergency Response Team/Coordination Center (CERT/CC), the Financial Services Information Sharing and Analysis Center (FS/ISAC), and the FBI.

-more-

This guidance, Bulletin 2000-14, can 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 1:00-3:30 p.m., Monday-Friday).

# # #

The OCC charters, regulates and examines approximately 2,400 national banks and 58 federal branches of foreign banks in the U.S., accounting for more than 57 percent of the nation's banking assets. Its mission is to ensure a safe and sound and competitive national banking system that supports the citizens, communities and economy of the United States.