

Committee on Government Reform

CONGRESSMAN TOM DAVIS, CHAIRMAN



NEWS RELEASE

For Immediate Release
September 24, 2003

Contact: David Marin
(202) 225-5074

Davis Introduces “Government Network Security Act of 2003”

Washington, D.C. – House Government Reform Committee Chairman Tom Davis (R-VA) today joined Ranking Member Henry Waxman (D-CA) in introducing the “Government Network Security Act of 2003,” bipartisan legislation that closes a loophole in the federal government’s efforts to protect the security and privacy of its computers.

The legislation requires federal departments and agencies to take steps to protect government computers and information from the risks posed by the use of peer-to-peer file sharing programs.

Peer-to-peer file sharing programs are Internet applications that allow users to download and directly share electronic files from other users on the same network. These programs are surging in popularity with millions of people trading music, images and documents over these networks at any given time.

“While most of the news coverage on file sharing focuses on the ability of users to illegally trade copyrighted music, movies, and videos, another less publicized dark side to this technology is the risk it poses to the security of computers and the privacy of electronic information,” Davis said. “Few people recognize these risks. Using these programs is similar to giving a complete stranger access to your personal file cabinet.”

At a May hearing held by the Committee on Government Reform, Members learned about the privacy and security risks created by these programs. Through a couple of simple searches on one file sharing program, Committee staff easily obtained tax returns, medical records, and confidential legal documents, and business files.

Needless to say, file sharing programs create a number of risks for federal departments and agencies if they are installed on government computers.

The federal government uses and stores a wide variety of classified and sensitive information, including information vital to national security, defense, law enforcement,

economic markets, public health, and the environment. Government computers also contain personal and financial information of U.S. citizens and businesses. **Installing these programs on government computers can expose this sensitive information to the public. It also creates the potential for the spread of viruses, worms, and other malicious computer files. The files downloaded using file sharing programs can also consume valuable network resources, which could result in a degradation of network performance.**

Both the House and Senate have successfully addressed these risks through both technical and non-technical means, including firewalls and employee training. This legislation would require the Executive Branch to take similar steps to protect its computers.

“File sharing technology is not inherently bad, and it may turn out to have a variety of beneficial applications,” Davis said. “However, as our Committee has learned, this technology can create serious risks for users. This bill takes a common sense approach to protect the computers and networks of the federal government and the valuable information they contain.”

###