COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
SEPTEMBER 25, 2003

FACT SHEET
H.R. 3159, the "Government Network Security Act of 2003"

The "Government Network Security Act of 2003" (H.R. 3159), introduced by Ranking Member Henry Waxman and Chairman Tom Davis, requires that federal agencies protect their computers and networks from the security risks posed by peer-to-peer file sharing. This fact sheet provides answers to basic questions about peer-to-peer file sharing programs, the security risks they pose, and H.R. 3159.

What are peer-to-peer file sharing programs?

Peer-to-peer (P2P) file-sharing programs are Internet applications that allow computer users to share electronic files with other users connected to a common file sharing network. P2P file sharing programs can be used to share any type of electronic files, but are commonly used to share music, movies, and video games.

P2P file sharing programs have become incredibly popular in recent years. One such program, Kazaa, has been downloaded nearly 280 million times – more than any other software program in Internet history. Other popular programs include BearShare and iMesh.

What security risks are associated with peer-to-peer file sharing programs?

P2P file-sharing programs increase the connectivity between computers connected to a common P2P network. This heightened connectivity can expose computers to risks beyond those raised by other Internet activities.

A user of a P2P file sharing program chooses which folders on his or her computer are available for sharing with others on the same P2P network. Because P2P file-sharing programs allow the sharing of any type of electronic data, every computer file in these shared folders becomes accessible to every other user on the P2P network. A P2P user who chooses to share a folder containing a music collection may not be aware that he or she is also sharing every personal document that might be stored in the same location.

A recent Government Reform Committee investigation found that P2P users are in fact sharing far more than movies, music, and video games. Using a simple search tool built into the Kazaa program, staff investigators found users sharing completed tax forms, medical records, and even complete e-mail inboxes.

This increased connectivity of P2P file sharing also means that the computers used to operate these programs can be at greater risk for viruses and other malicious files. At a May 2003 Government Reform Committee hearing, leading network security experts testified on how viruses and worms can multiply on these P2P networks and enter into a user's computer through a P2P file sharing program.

What security risks do P2P file sharing programs pose for federal government computers?

The security risks of P2P file sharing programs potentially become far more serious when federal government computers are used to connect to P2P networks. The electronic information exposed may include data vital to national security and personal files about citizens such as financial, military, and medical records. P2P use on even one computer can introduce viruses and worms to critical government networks, potentially slowing the functioning of the affected agency.

The United States House of Representatives and Senate recognized the risks of peer-to-peer file sharing nearly two years ago. The House and Senate are successfully protecting the privacy and security of congressional computers from the risks of P2P file sharing through firewall technologies and employee policies on appropriate computer use.

Although Congress has addressed the risks of P2P file sharing, many federal government agencies have not taken the steps necessary to protect their networks and computers. An ongoing GAO investigation requested by the Government Reform Committee has found computers actively using peer-to-peer file sharing at federal agencies entrusted with sensitive government information, including a Department of Energy nuclear laboratory, the headquarters of the Department of Labor, and a facility that manages NASA's space flight research.

What does H.R. 3159 do?

H.R. 3159, the "Government Network Security Act of 2003," requires that federal agencies address the security risks posed by P2P file sharing programs when developing their network policies and procedures. Agencies must ensure that federal computers and the important information they store remain secure, private, and protected, but agencies are given the flexibility to develop the most appropriate means of accomplishing this goal through a combination of technological means (such as firewalls) or nontechnological means (such as employee training).

Under H.R. 3159, each agency will have six months in which to develop and implement a plan for protecting their computers from the security risks posed by P2P file sharing. Within the following year, GAO must review these plans and report back to Congress on their adequacy and effectiveness.

The "Government Network Security Act" does not hinder the ability of federal agencies to pursue new advances in technology, including peer-to-peer technologies needed for government applications. It requires only that in pursuing these innovations, agencies not put at risk the security of government files.