

TOM DAVIS, VIRGINIA,
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTIS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
WILLIAM J. JANKLOW, SOUTH DAKOTA
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051
TTY (202) 225-6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT,
INDEPENDENT

Statement of Rep. Henry A. Waxman, Ranking Minority Member Committee on Government Reform Business Meeting on H.R., 3159, The Government Network Security Act of 2003

September 25, 2003

Today we are considering the Government Network Security Act. This is legislation that Chairman Davis and I have worked closely together to develop. It addresses computer security threats posed by the growing popularity of Internet file-sharing programs.

In recent years peer-to-peer file-sharing programs have gone from little known to incredibly popular Internet applications. In fact, the most popular of these file-sharing programs, Kazaa, has been downloaded more than 280 million times – making it the most downloaded software program ever.

In a series of hearings earlier this year, this Committee looked into these peer-to-peer file-sharing programs and the issues they raise. What we found out is that the risks they pose – particularly to our personal privacy and security – can be significant.

At a Government Reform Committee hearing in May, we heard from leading network security experts from universities and the private sector about how peer-to-peer file sharing can put computers at risk from viruses, worms, and other damaging computer files.

And a Committee investigation found that without even knowing it, people are sharing incredibly personal information through these programs. Our staff investigators found completed tax returns, medical files, and even entire e-mail inboxes being shared on these networks.

Government computers are not immune from these risks. A GAO investigation, which is still underway, has found that even at Los Alamos National Laboratory, where top secret research is often conducted, file-sharing programs have been found on government computers.

Protecting government computers from these security risks is essential. The federal government has computer records with incredibly sensitive personal information about citizens, including tax returns, military records, and medical and psychiatric records. It also obviously has many files with important national security information.

It is also important to protect government computers from computer viruses. In recent weeks we've seen how the spread of just two or three malicious viruses can slow the functioning of government. We need to make sure federal government computers and networks stay protected from these threats.

It is not difficult to safeguard federal computers from these risks. The House of Representatives recognized the privacy and security threats posed by peer-to-peer programs nearly two years ago and took steps to protect against them. The Senate did the same shortly after. But many of our federal agencies have yet to follow suit.

The Government Network Security Act of 2003 is simple legislation. It requires that when developing their network security policy and procedures, federal agencies address the risks posed by peer-to-peer file sharing programs. Plans to address these risks may include technological means (such as firewalls) and nontechnological means (such as employee training).

Technical innovation is tremendously important. The Government Network Security Act recognizes this, and it protects the ability of federal agencies to pursue new technologies, including peer-to-peer technology. The only limitation it imposes is the requirement that agencies not jeopardize the security of sensitive government records.

When popularly available peer-to-peer file sharing programs can threaten us with viruses and worms and put at risk the privacy of sensitive information, I think that we can all agree that they have no place on government computers and networks. That's why I urge my colleagues to support this legislation.