UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

MAY 21 2004

MEMORANDUM FOR: Heads of Operating Units
Chief Information Officers

FROM: Thomas N. Pyke, Jr.

SUBJECT: Commerce IT Security Policy on Peer-to-Peer File Sharing

Recent increased public concern about unauthorized use of Government computers, including use of public peer-to-peer (P2P) technology, coupled with reports of possible unauthorized use of Government computers involving P2P technology in two of our Operating Units, led to this IT Security policy addendum. This addendum includes standards and controls for determining unauthorized use, prevention of unauthorized use, and monitoring for unauthorized use. Enforcement of this policy is effective immediately.

What is P2P technology?
P2P technology refers to any software or system that allows individual users of the Internet to connect (directly, through the Internet) to each other so as to transfer or exchange computer files. The definition used by the Federal Enterprise Architecture is that P2P technology is a class of applications that operates outside the Internet Domain Name Service (DNS) system, that has significant or total autonomy from central servers, and that takes advantage of resources available on the Internet.

What is the Commerce policy regarding P2P technology?
The attached addendum to the Commerce *IT Security Program Policy* states that Commerce prohibits unauthorized P2P file sharing technology from use on Commerce IT systems unless it has been explicitly authorized in writing by an operating unit CIO in support of an official Commerce IT application.

Why is the Department of Commerce concerned about P2P technology?
P2P technology, when misused, can lead to possible copyright infringement or the appearance of copyright infringement by employees. It may even appear that an entire organization is culpable, unless special attention has been given by the organization to preventing such actions. The use of public P2P technology is potentially much worse than a user simply downloading files from a system somewhere on the Internet. Users of P2P technology may (even unknowingly or unintentionally) be supporting file sharing by others due to the capabilities of the downloaded public P2P software. There are significant additional IT security risks associated with public P2P technology, as noted below. These concerns are in addition to loss of employee productivity by downloading and listening to or watching the content of such files and the use of Government network and computing resources while doing so.

The Department of Justice told the Federal CIO Council that "such systems are highly decentralized and are designed to facilitate connections between persons who are looking for certain types of files. The vast majority of files that are traded on P2P networks are copyrighted

music files." The use of publicly available P2P software for purposes such as this is referred to as "public" P2P technology.

In addition, the Department of Justice informed us that many of the software packages downloaded by users to support their involvement in sharing files using public P2P technology can also be set up to make files on a user's computer accessible to large numbers of people on the Internet. Some of these files, if they have been copied from other users' systems on the Internet using P2P technology, may represent copyright infringement or the appearance of copyright infringement. Making them available on a Commerce computer for copying by users on the Internet may also result in copyright infringement. In addition, people who use P2P technology not only may be sharing music and other files illegitimately over the Internet but also inadvertently sharing the entire contents of the hard drive on their computer.

How does this addendum relate to existing Commerce IT Security and Internet Use Policies?

The addendum complements the existing Commerce *IT Security Program Policy* and the *Internet Use Policy,* which define employee responsibilities, authorized use of Commerce IT systems, and outline the management, operational, and technical control minimum standards to protect Commerce systems. These policies include the following sound IT security practices and may help prevent unauthorized use of P2P technology:

Operating Unit Heads must ensure that the operating unit has an established IT Security Program and ensure adequate resources are provided to implement IT security activities. The program must include mechanisms to educate Commerce personnel regarding IT security policies and procedures and must address the consequences of policy violations, such as those imposed under Department Administrative Order 202-751, *Discipline* (found at http://www.osec.doc.gov/omo/daos/202-751.htm).

Program Officials must support the process of system accreditation, which verifies and validates the adequacy of system security controls, and authorize systems to operate in support of the Commerce mission.

System Owners must develop system security plans that address adequate system security measures, to include:

- Establishing rules of behavior for system users, including remote users.
- Configuring firewalls that protect systems on Commerce internal networks to close ports not required for official Commerce IT applications. Through an established system configuration management process (ideally including a review by the operating unit IT security office), the system owner must approve port use in writing (with the exception of ports 80 and 443).
- Configuring network devices such as firewalls, routers, and intrusion detection systems to filter incoming and outgoing traffic such as unauthorized P2P transmissions that may be port-sensitive.
- Monitoring network performance.
- Logging unusual activity and attempts of P2Ptransmissions where they can be detected.
- Supporting the enforcement of consequences for unauthorized use of P2P technology by Commerce personnel.

- Ensuring certification testing of all system controls to validate their effectiveness and ensuring accreditation of systems to establish accountability for system security.

The Commerce *IT Security Program Policy and Minimum Implementation Standards (IT Security Policy)* can be viewed on the Web at

http://www.osec.doc.gov/cio/oipr/ITSec/DOC-IT-Security-Program-Policy.htm

All personnel (including federal employees, contractors, guest researchers, collaborators, and others) are expected to comply with published rules for ethical behavior and for acceptable system use, including those established by the Commerce *Internet Use Policy* (found at http://home.commerce.gov/Internet_use_policy.htm). In addition, the recently issued, revised Commerce Internet Use Policy prohibits 1) Internet use that could generate or result in an additional charge or expense to the Government and 2) participation in or encouragement of illegal activities or the intentional creation, downloading, viewing, storage, copying, or transmission of illegal or discriminatory materials.

What should Commerce operating units do to address the Department's concerns with P2P technology?

Please review your operating unit policies and procedures to ensure they are aligned with this policy addendum. If you have questions, please contact Nancy DeFrancesco, the Department's IT Security Program Manager, at (202) 482-3490.

Addendum to the Department of Commerce IT Security Policy
Restrictions on the Use of Peer-to-Peer (P2P) File Sharing

This addendum to the Commerce *IT Security Program Policy* applies to all classified national security and unclassified Commerce systems used to process and store Commerce information, and to all Commerce operating units and personnel (federal and contractor), guest researchers, collaborators, and others requiring access to the hardware and software components of any Commerce IT systems. It also requires implementation of specific controls to protect Commerce IT systems from compromise, as well as controls to prevent, detect, and respond to unauthorized activity. The following policy statement and the specified minimum standards and controls are intended to prevent and detect unauthorized use of Peer-to-Peer (P2P) technology.

The Department prohibits use of P2P file sharing technology on any Commerce IT system unless it has been explicitly authorized in writing by an operating unit CIO in support of an official Commerce IT application. A copy of each such authorization shall be sent to the Commerce CIO. In implementing this policy, CIOs must give special attention to ensuring that public P2P technology is not being used to support sharing of computer files that contain music, digital film, TV shows or other information such that copying of the files may infringe on any copyrights or other associated intellectual property restrictions.

Operating unit CIOs shall be especially careful that any of the following **public online** file-sharing services, or similar services, designed to facilitate the sharing of computer files (including music, digital film, and TV shows) are not used on any Commerce IT system in such a way as to potentially infringe on copyrighted material:

1stWorks, AudioFind, BadBlue, BearShare, Blubster, CareScience, Clip2, DirectConnect, FastTrack, Fatbubble, File Rogue, Filetopia, FreeWire, Frontcode Technologies, FurthurNet, Gnotella, Gnutella, Grokster, Harmonic Invention Software, Hotline Connect, iMesh, Ionize, Jibe, Jungle Monkey, KaZaA, LimeWire, MangoSoft, Morpheus, Myster, NextPage, Inc., Ogg Vorbis, Ohaha, OnSystems, OpenNap, Pointera, Radio Userland, Rapigator, Shareaza, Softwax, Songbird, SongSpy, Spinfrenzy.com, Splooge, Streamcast, Swaptor, Thinkstream, Toadnode.com, LLC, Tripnosis, Inc., Vitaminic, WebDAV.

Commerce CIOs should ensure that system owners **uninstall unauthorized P2P software** and that they implement adequate controls to prevent it from being installed and used on Commerce computers, including use of administrative and technical means to:

- Limit the ability of Commerce internal network users to load software themselves on computers. This control concept can be supported by the use of automated software patching tools and centralized oversight of large numbers of computers in an automated manner, while maintaining tight configuration control over all computers.
- Evaluate and implement cost-effective mechanisms to monitor and detect unauthorized P2P activity within Commerce networks.
- Communicate P2P awareness information to internal network users and to remote users (such as teleworkers and researchers processing and storing Commerce data on personally-owned computers).

This addendum to the Commerce *IT Security Program Policy* is authorized by Tom Pyke, Commerce CIO, is effective on May 21, 2004, and will remain in effect until incorporated into the next update of the Commerce *IT Security Program Policy.*