Exhibit 10.8.27-1 (03-31-2008)
Prohibited Uses of Government IT Resources

Prohibited uses of Government IT resources includes, but is not limited to, the following examples:

Note:

These examples and other prohibited uses are in affect regardless of work status.

1) The creation, copying, transmission, download, or retransmission of greeting cards, video, sound (including streaming video or music), other files larger than 1 megabyte, or the use of e-mail practices that involve ongoing message receipt and transmission (referred to as instant messaging/messenger). "Push" technology on the Internet (e.g., subscribing to any unofficial service such as EntryPoint or LaunchPad) that gathers information and sends it out automatically to subscribers) and other continuous data streams (such as streaming stock quote);

2) Using Government IT resources for personal communication on blogs and social networking sites such as MySpace, Facebook, Friendster, Xanga, hi5, Orkut, Yahoo! 360°, Cyworld, Bebo, XuQa, etc.;

3) Access to pornography or hacker sites (sites which open the IRS to unacceptable security risk) regardless of the security risks or lack thereof;

4) Using Government systems as a staging ground or platform to gain unauthorized access to other systems;

5) The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter;

6) Using Government IT resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation;

7) The creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials, including web sites classified as Personals & Dating;

8) The creation, download, viewing, storage, copying, or transmission of materials related to gambling (legal and illegal), illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited, etc.;

9) Downloading, copying, and/or playing of computer video games;

10) Downloading, copying, or installing of unauthorized data programs (e.g., executable code), such as screen savers, software products, or copyrighted materials such as music and pictures (*See Exhibit 10.8.27-2* for an additional explanation of an unauthorized program);

11) The use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services);

12) Engaging in any political fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity, in accordance with, Title 5 - Code of Federal Regulations (CFR) - Part 735, Office of Personnel Management, Employee Responsibilities and Conduct.

13) The use for posting agency information to external news groups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate agency written approval has been obtained or the use is not at odds with the agency's mission or positions;

14) Any use that could generate more than minimal additional expense to the Government (e.g., subscribing to unofficial LISTSERV or other services which create a high-volume of e-mail traffic);

15) The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information; material which is copyrighted, trademarked, or otherwise controlled with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data;

16) The use of peer-to-peer (P2P) file sharing and networking. P2P refers to any software or system allowing individual users of the Internet, intranet or extranet to connect and share files or resources. Specific examples of P2P file sharing include applications such as Morpheus, Napster, Grokster, Kazaa, Gnutella as well as decentralized applications such as SETI@Home. P2P is not allowed and is considered outside the scope of limited personal use. Furthermore, engaging in P2P creates a substantial computer security risk in that P2P may facilitate the spread of computer viruses.

17) Any personal use or storage of files on Home Directories or other network drives provided and maintained by the IRS;

18) Any use that reduces employee productivity or interferes with the performance of official duties;

19) Any access to non-IRS e-mail accounts through the Internet (i.e., accessing personal AOL accounts, accessing company accounts, etc. through the IRS Internet firewall);

20) Any access to the Internet that does not go through an IRS-approved Internet gateway (i.e., firewall). Accessing the Internet from non-office locations using a government-owned computer must always be done via the IRS-approved internet gateway; using any other connection (such as a private AOL account) is prohibited;

21) Any access to an Internet site that contains similar content to sites which have been prohibited or restricted.

22) Any use of a photocopier or fax machine that involves more than a few pages of material (e.g., copying a book, making numerous copies of a resume, or sending/receiving a lengthy document via fax machines); and

23) Any use of photocopiers or fax machines that conflicts with the need to use the equipment for official business requirements.

24) Any use of telephone services that creates more than minimal additional expense to the Government.

Employees should also remember that some use of Government IT resources is absolutely forbidden, even during non-work hours.