In Reply Refer to:
1264 (OR-955) P

November 19, 2002

EMS TRANSMISSION
Instruction Memorandum No. OR-2003-017
Expires: 9/30/2004

To: DMs, DSDs, Staff and Branch Chiefs
   Attention: IRMs

From: State Director

Subject: Use of Personally Owned Computing Devices for BLM Work

This directive addresses a long-standing policy that personally owned equipment may not be used for Government work. As the availability of personally owned computing devices including PCs, hand-helds, and PDAs, becomes more prevalent in employees' homes, and flexible workplaces become a more common practice, it is important to note this policy.

The issues associated with allowing employees to perform BLM work on personally owned computing devices are complex. The convenience to the employee must be balanced with security, liability, and other potentially costly concerns. The policy is that personally owned computing devices or other personally owned information technology, are not to be utilized to perform Bureau work. Oregon/Washington offices must provide employees the information technology that they require to perform their duties whether they are working in the office or off site. Some of the information resources management issues associated with the use of personally owned computing devices are:

- Bureau owned applications and software may not be installed on personally owned computing devices.
- The Bureau is not staffed to provide technical support for personally owned equipment.
- Personally owned equipment conforms to no standards or minimum configurations to assure it can perform Bureau functions and protect Bureau data.
- Conversion of data from home based applications to Bureau applications frequently requires considerable effort to research solutions and can result in lost data.
- Viruses could be introduced to Bureau systems from the exchange between personal and BLM equipment through a floppy diskette, a login session on the remote access server or synching with a government furnished PC.

- Personally owned equipment is not required to provide Bureau recoverable backup capability.
- Since personally owned equipment is typically for family use, the potential for loss, compromise, or inappropriate release of data is a serious concern.
- Should an employee fail to return to work for any reason, it may be difficult for the Bureau to recover its data from personally owned equipment.
- Since nonpublic data is not released outside the agency and cost recovery principles are in place for other data,
the potential for transfer of data from a personally owned computing device to the public could compromise our efforts to protect the data (e.g., especially sensitive data such as cultural site and endangered species locations, IITD data, Privacy Act information such as mailing addresses, or proprietary information).

Questions about this policy may be referred to Cynthia Yee, OR/WA IT Security Manager, OR955.1, Branch of Information Resources Management, at (503)808-6117, or via e-mail.

**Districts with Unions** are reminded to notify their unions of this IM and satisfy any bargaining obligations before implementation. Your Servicing Personnel Office or Labor Relations Specialist can provide you assistance in this matter.

Signed by: Kathy J. Eaton  
Acting Associate State Director  

Authenticated by: Mary O'Leary  
Management Assistant

Distribution: WO500 (5640, MIB)