Memorandum
OHSU Integrity Office
Mail code AD 140
3181 SW Sam Jackson Park Road
Portland, OR 97239-3098

March 14th, 2007

FROM: **Ronald Marcum, MD**
Chief Privacy Officer
Chief Information Security Officer
Chief Medical Information Officer

SUBJECT: Verification of OHSU Compliance with the Federal Information Security Management Act of 2002 (FISMA)

Purpose

The purpose of this memorandum is to communicate Oregon Health & Science University's enterprise security control baselines with regard to FISMA. Although OHSU is not a federal agency and, therefore, not explicitly subject to FISMA, we have undertaken an evaluation of our existing information privacy and security program versus the standards defined in National Institute for Standards and Technology (NIST) Special Publication 800-53, Revision 1 (http://csrc.nist.gov/publications/nistpubs/).

Conclusions

1. OHSU's information security controls for enterprise information systems meet the control baselines for low-impact systems as detailed in *Recommended Security Controls for Federal Information Systems, Low-Impact Baseline* NIST Special Publication 800-53, Revision 1, Annex 1 (http://csrc.nist.gov/publications/nistpubs/).
2. Some of the specific controls specified in the low baseline are exceeded by OHSU due to our own risk management decisions (which are made based on criteria beyond the scope of FISMA). In these instances, specific controls often meet the standard for moderate-impact or high-impact systems.
3. Some of the specific controls specified in the low baseline are not fully implemented, but have been identified as part of our security plan (analogous to the POA&M required under FISMA).
4. These conclusions apply to OHSU enterprise-managed systems. OHSU users who receive, create, or maintain electronic information are responsible for ensuring that the information is stored only in systems that provide appropriate security controls. In instances where non-enterprise-managed systems (e.g., departmental servers, removable storage devices, standalone laptops and other portable media) the Steward of these systems will need to be individually consulted to verify control baselines.

Further clarification can be obtained by contacting the OHSU Office of Information Privacy and Security at oips@ohsu.edu or (503)494-8849.