OREGON HEALTH & SCIENCE UNIVERSITY

Memorandum

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

March 13th, 2007

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

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

Background

The Federal Information Systems Security Act of 2002 (FISMA) establishes responsibility and accountability for the security of all federal agency information systems. The National Institute for Standards and Technology (NIST) was tasked with establishing the detailed standards to support this law and these standards are defined in NIST Special Publication 800-53, Revision 1 (http://csrc.nist.gov/publications/nistpubs/). The NIST standards establish 171 separate "controls" that may be required for information systems (depending on the sensitivity level of the system). The NIST standards require that federal agencies confirm that any outside entity receiving federal information subject to FISMA maintain it appropriately in accordance with FISMA standards. As a result of these requirements, federal agencies providing information to OHSU are asking for confirmation of OHSU's compliance with FISMA standards.

Purpose

The purpose of this memorandum is to provide OHSU users with guidance for responding to inquiries regarding OHSU's compliance with FISMA. OHSU is not a federal agency and is, therefore, not explicitly subject to FISMA. OHSU is, however, subject to other legislation that requires similar reasonable information security safeguards. The safeguards implemented on OHSU's centrally managed enterprise systems provide adequate assurances of confidentiality, availability and integrity for our various missions. Information Stewards are ultimately responsible for ensuring that they store information within the appropriate systems at OHSU. Outside of the centrally managed enterprise systems, individual Stewards and Users are responsible for ensuring that these same safeguards are established and maintained, as appropriate, for the information they maintain.

Guidelines

OHSU users may respond to these requests by providing an overview of OHSU's relevant security controls that are established for the involved enterprise information systems. A detailed summary of OHSU's enterprise security program should not be necessary for any federal agency to collaborate with OHSU, however it is appropriate to affirm that OHSU meets the *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/).

For non-enterprise-managed systems (e.g., departmental servers, removable storage devices, standalone laptops and other portable media) the Steward of these systems is responsible for assuring that OHSU information security standards are met. These standards are available on the OHSU intranet (http://ozone.ohsu.edu/cc/sec/isp/). FISMA compliance questions relating to these systems must be addressed by the individual Stewards and Service Providers for these systems. The OHSU Office of Information Privacy and Security is available for assistance.

Presently, the Department of Veterans Affairs Medical Centers (VAMCs) appears to be particularly interested in security controls related to confidentiality of information. Accordingly, users collaborating with VAMCs (e.g., investigators, research coordinators) should pay particular attention to OHSU policies relating to:

- Secure Storage of Electronic Restricted Information (http://ozone.ohsu.edu/cc/sec/isp/00006.pdf)
- Secure Transmission of Electronic Restricted Information (http://ozone.ohsu.edu/cc/sec/isp/00007.pdf)
- Access Authorization to Electronic Restricted Information (http://ozone.ohsu.edu/cc/sec/isp/00009.pdf)
- Physical Safeguards for Computing Devices & Electronic Media (http://ozone.ohsu.edu/cc/sec/isp/00012.pdf)
- Information Security Incident Reporting Procedures (http://ozone.ohsu.edu/cc/sec/isp/00017.pdf)

Federal agencies and OHSU users requiring further clarification regarding this guidance should contact the OHSU Office of Information Privacy and Security at oips@ohsu.edu or (503)494-8849.