Smithsonian Institution
Office of the Inspector General

In Brief

Smithsonian Institution Information Security Program

Report Number A-10-01, March 15, 2011

Why We Did This Audit

The Federal Information Security Management Act of 2002 (FISMA) directs the Office of the Inspector General to annually evaluate the information security program of the Institution. The Institution voluntarily complies with FISMA requirements because it is consistent with its strategic goals. We hired an independent auditor to conduct this review on our behalf.

What We Recommended

The independent auditor made five recommendations to improve the Institution's systems inventory and to ensure that portable computers and mobile devices that may store sensitive information are secured with appropriate encryption technology.

Management concurred with the report findings and recommendations.

What We Found

The independent auditor assessed Smithsonian Institution and Smithsonian Enterprises policies and procedures against federal information security policies and guidance. They met with the Smithsonian Institution's and Smithsonian Enterprises' senior IT security management staff, and SI FISMA system points of contacts.

Testing was limited to those major systems included in the Institution's FISMA inventory and, at our request, Smithsonian Enterprises systems that were subject to Payment Card Industry Data Security Standards, although those systems are not subject to FISMA and are not part of the Institution's FISMA inventory. With the exception of the Smithsonian Astrophysical Observatory, these systems were primarily hosted by the Office of the Chief Information Officer (OCIO) at the Smithsonian Data Center and Smithsonian Enterprises.

The independent auditors identified control deficiencies in how management identifies systems to be included in the FISMA Inventory, and operational deficiencies in applying encryption technology to portable computers and mobile devices that may be used to store sensitive information. Specifically, they determined that:

- The method used for determining the FISMA inventory was not based on a risk analysis that assessed all risk elements as found in applicable NIST standards and publications.
- The Institution was not effectively identifying laptops that store sensitive information and applying the appropriate encryption technology.

For additional information, contact the Office of the Inspector General at (202) 633-7050 or visit http://www.si.edu/oig.