Smithsonian Institution
Office of the Inspector General

In Brief

Smithsonian Institution Research Information System
Report Number A-09-02, June 12, 2009

Why We Did This Audit

Under the Federal Information Security Management Act of 2002 (FISMA), the Office of the Inspector General conducts an annual independent assessment of the Institution's information security system. As part of that assessment, FISMA requires a review of a subset of information systems. This report covers one such system, the Smithsonian Institution Research Information System (SIRIS), and evaluates management, operational, and technical security controls.

What We Recommended

We made 3 recommendations to strengthen controls over the SIRIS application by ensuring that librarians do not enter sensitive personally identifiable information such as social security numbers into the SIRIS application; that management identifies, documents, and implements a baseline for the SIRIS database; and that management reviews and updates the system security plan to include accurate descriptions of the controls in place or planned.

Management concurred with our findings and recommendations and has planned actions that will resolve all our recommendations.

What We Found

SIRIS is an Institution-wide system for both public and scholarly research. It applies established national standards to manage, describe, and provide access to information resources held primarily by the Institution's libraries, archives, and research units in support of the Institution's mission.

Overall, we determined operational, management, and technical controls for the SIRIS application were substantially in place and operating effectively. While management has complied with the majority of Institution, OMB, and NIST requirements, we did identify three areas where management needs to implement improvements. Specifically, we found that:

- Librarians entered social security numbers into SIRIS, against established policy and without management's knowledge, increasing the risk that this information may be inappropriately accessed and used by unauthorized personnel.

- Management has not developed or implemented a security configuration baseline for the SIRIS database. Instead, management uses the default configuration settings, which may not adequately protect the system.

- Finally, the SIRIS security plan does not accurately describe all controls in place. Without adequate or accurate descriptions of controls, management may be unaware of security risks to the system.

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