Smithsonian Institution
Office of the Inspector General

In Brief

Smithsonian Institution Information Security Program Evaluation, Report Number A-09-11, June 30, 2010

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 Smithsonian Institution's information security controls. As part of that assessment, FISMA requires a review of the Institution's Security Management Program and an evaluation of associated management, operational and technical security controls. An independent auditor conducted this review on our behalf.

What We Recommended

We made one key recommendation to reassess the security categorization for major systems currently categorized as low-impact systems, based on the type of personally identifiable information stored in the system. These systems should either be re-classified as moderate or the security categorization revised to include adequate justification for classifying the system as low.

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

What We Found

During the past year, the Office of the Chief Information Officer (OCIO) made improvements to strengthen their information security program. Specifically, OCIO:

- Enhanced the tracking of Certification and Accreditation (C&A) artifacts, Plans of Actions and Milestones, and quarterly compliance via a FISMA scorecard.
- Improved security training by reviewing security program practices with Senior Executives and Management staff, and by conducting risk management briefings with Mission and System Sponsors.
- Improved all major systems security plans and clarified C&A boundaries.
- Developed a standardized Security Test and Evaluation (ST&E) Plan and a Security Assessment Reporting (SAR) format across all major systems to include clear identification of inherited common controls unique to each system.

However, we identified one key objective that we believe management had not substantially completed. We recommended reassessing the security categorization for major systems currently categorized as low-impact systems, based on the type of personally identifiable information stored in the system. These systems should either be reclassified as moderate or the security categorization revised to include adequate justification for classifying the system as low.

We also recommended that computer security incidents be reported to the United States Computer Emergency Readiness Team (US-CERT) within the required timeframe of the type of incident and that that all interconnections have signed agreements prior to implementation.

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