Smithsonian Institution
Office of the Inspector General

In Brief

Information Security Practices
Report Number A-08-09, March 17, 2009

Why We Did This Evaluation

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 they are consistent with its strategic goals. During this year's review, we assessed (1) the effectiveness of the Institution's security program, (2) the Institution's compliance with FISMA guidelines, (3) the National Museum of Natural History Electronic Museum application and the Smithsonian Astrophysical Observatory Scientific Computing Infrastructure, and (4) progress made in correcting previously reported information security weaknesses.

What We Recommended

We made 10 recommendations to ensure that policies address general security awareness training for all personnel; the Federal Desktop Core Configuration requirements are implemented; OIG findings are included on system POA&Ms; management will re-assess the risk of consolidating major systems within a single accreditation boundary; development of E-authentication risk assessments for non-major systems; and the Institution requires signatures on all C&A documents.

Management generally concurred with the report findings and recommendations.

What We Found

While the Institution has made progress in complying with information security requirements, additional work remains to ensure adequate controls are in place and operating effectively. Specifically, we found that:

- The Institution did not require general security awareness training for employees, contractors, volunteers, visiting scholars, and interns with no computer or network access. Without requiring such training for all personnel, the Institution cannot ensure that the collection, processing, maintenance, transmission, and dissemination of information in both electronic and non-electronic forms are appropriate.

- The Institution has not fully implemented Federal Desktop Core Configuration (FDCC) requirements over its desktop and laptop hardware. Without fully implementing FDCC, the confidentiality, availability, and integrity of Institution systems and related data may be at greater risk than management is willing to accept, and the Institution may not fully achieve the performance, cost, and security benefits of the FDCC settings.

- Plan of Action and Milestones (POA&M) did not include all information required by Institution and OMB policies. Without a complete POA&M, system sponsors and OCIO cannot effectively track and remediate weaknesses, which may cause unnecessary vulnerabilities in the system that could lead to a loss or compromise of data within the system.

- When management consolidated multiple systems into a single accreditation boundary, it did not conduct a revised risk assessment and update the system security plan to reflect the common controls in place for all systems or the unique controls for each system. Because the systems were not subject to a revised risk assessment, there were no annual control assessments completed.

- Management has not completed an e-authentication risk assessment nor has it performed an initial assessment of the Institution's web presence to identify the types of information collected. Without such assessments, management cannot ensure adequate protection of public users' identities.

- Finally, management did not properly sign certification and accreditation documentation. Unless documented policies and procedures are followed, management cannot ensure that adequate controls are in place, which may cause vulnerabilities in the system.

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