Smithsonian Institution
Office of the Inspector General

In Brief

Information Security Practices
Report Number A-07-08, March 31, 2008

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 it is 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 security of the Human Resources Management System and ID and Badging, C-Cure Central, and Central Monitoring Systems, and (4) progress made in correcting previously reported information security weaknesses.

What We Recommended

We made four recommendations to ensure that controls over major and minor systems are identified, documented, and implemented; system sponsors report their progress on remediating security weaknesses and that system specific POA&M activities are consolidated in the agency-wide POA&M; and policies and procedures for conducting annual security control testing are developed, documented, and implemented.

Management concurred with the report's findings and recommendations and has planned actions that will resolve all our recommendations.

What We Found

While progress has been made 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's certification and accreditation process did not identify all major and minor systems in accordance with National Institute of Standards and Technology and FISMA requirements. Specifically, while management has certified and accredited portions of the Security Management System, it did not include other associated sub-systems and components. In addition, management did not include or address other Institution information systems in any of the Institution's system security plans.

- The Office of the Chief Information Officer (OCIO) did not centrally track, review, and consolidate system plan of action and milestones (POA&M) activities into the Institution-wide POA&M on a quarterly basis in accordance with Institution policy. While OCIO did report an Institution-wide POA&M to OMB on a quarterly basis, the submission did not include or consolidate all system POA&M items. Moreover, program officials did not consistently report the status of findings and recommendations reported in system POA&Ms to the CIO on a regular basis.

- Management did not ensure results of annual security control testing were adequately documented and weaknesses were included in related POA&Ms for tracking and correction. Specifically, OCIO has not developed and documented a policy or procedures specifying how management should determine what controls to test and what minimum documentation should be produced to support testing. A lack of adequate documentation to support the results of annual testing diminishes management's assurance that controls were adequately tested and that conclusions based on test results were appropriate. In addition, a lack of appropriate documentation of test results increases the risk that identified weaknesses will not be included in the system POA&M for tracking corrective actions.

We again note that the Institution's decentralized IT environment makes the implementation and enforcement of policies and procedures limited or inconsistent. Without the centralization of IT operations and the assignment of responsibility within OCIO for ensuring Institution policy and procedures are being followed, management cannot ensure adequate controls are in place.

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