Smithsonian Institution
Office of the Inspector General

In Brief

Privacy Program
Report Number A-08-08, May 29, 2009

Why We Did This Evaluation

We conducted an audit of the Smithsonian Institution's privacy and data protection policies, procedures, and practices to determine whether the Institution effectively handles privacy information.

What We Recommended

We made 11 recommendations to strengthen controls over private information by clearly defining the responsibilities of the Senior Agency Official for Privacy; developing, documenting, and implementing a comprehensive privacy program to include the collection, use, storage, disclosure, and safeguarding of sensitive PII and to reduce excessive PII; establishing privacy training; conducting privacy impact assessments and posting them on websites; and alerting staff to the importance of properly securing PII.

Management generally concurred with our findings and recommendations.

What We Found

The Smithsonian needs to significantly improve its policies, procedures, and practices related to the identification, collection, processing, and safeguarding of sensitive personally identifiable information (PII). While the Smithsonian has addressed limited privacy considerations, the measures it has taken are generally limited in scope, decentralized, and ultimately ineffective. Specifically, we found that:

- The Institution has not defined the responsibilities of the Senior Agency Official for Privacy (SAOP) to develop and implement a privacy program. Additionally, the SAOP should have competencies in the legal, security, and compliance aspects of privacy and, through hands-on involvement, be able to enforce policy.

- The Institution has not developed, documented, and implemented privacy policies and procedures for the identification, collection, use, storage, disclosure, on safeguarding of sensitive PII.

- Not all Smithsonian employees and contractors with access to PII understand privacy risks and their responsibilities for appropriately safeguarding PII.

- The Institution has not formalized procedures for conducting privacy impact assessments (PIA). Management acknowledges that, due to a backlog, it has not posted many completed PIAs on the Smithsonian website.

- Finally, management did not ensure that physical controls over sensitive PII were in place.

Without taking these actions the Institution leaves itself vulnerable to unnecessary or excessive privacy-related risks, such as that sensitive PII will be inappropriately collected, processed, or stored.

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