Smithsonian Institution
Office of the Inspector General

In Brief

Audit of the Smithsonian Institution's Privacy Program

Report Number OIG-A-16-4, March 14, 2016

What OIG Did

The Office of the Inspector General (OIG) contracted with an independent public accounting firm, Cotton & Company, to conduct this performance audit. The objective of the audit was to assess the effectiveness of the Smithsonian Institution's (Smithsonian) privacy program and practices.

Background

New privacy threats emerge daily, and the evolving nature of these threats makes it challenging to continually evaluate the measures needed to address risks to personally identifiable information. The increasing mobility of data significantly escalates the already difficult task of identifying where sensitive personally identifiable information is located and effectively securing it. Digital issues are not the only threat; about a quarter of the data-leakage incidents reported by large agencies involved the loss of sensitive information from hard copies or printed materials.

Due to these challenges and because it operates in a decentralized environment, it is critical for the Smithsonian to have a well thought out and comprehensive privacy program in place.

What OIG Found

Cotton & Company found that the Smithsonian has made progress in privacy management since the last OIG privacy audit in May 2009. For example, in 2014 the Smithsonian hired a new Privacy Officer, implemented a new privacy policy, and formed working groups to identify and address privacy issues.

However, Cotton & Company determined that significant work is still needed to institute key privacy processes and controls. For example, key activities that have not been completed include developing an organization-wide privacy strategic plan and documenting a comprehensive list of personally identifiable information being collected, processed, and stored throughout the Smithsonian. Without a clear understanding of the types of personally identifiable information being handled, management officials do not have reasonable assurance that they are collecting only the information needed to carry out the Smithsonian's mission and are adequately protecting that information from unauthorized use or disclosure. Additionally, Cotton & Company noted that the Smithsonian Privacy Office consists of one employee, the Privacy Officer, who supports 6,373 employees, 721 research fellows, and 9,817 volunteers.

To improve the privacy program, Cotton & Company found that:

- The Smithsonian needs a strategic privacy plan,
- The Smithsonian needs to develop a comprehensive inventory of personally identifiable information,
- The Smithsonian's privacy impact assessment process needs improvement,
- The Smithsonian's security awareness and privacy training need improvement,
- The Smithsonian needs to improve physical controls over personally identifiable information, and
- The Smithsonian needs to review and update privacy policies.

What OIG Recommended

Cotton & Company made 11 recommendations to address the findings listed above. Smithsonian management concurred with the recommendations and has proposed corrective actions to address them.

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