

**Privacy Impact Assessment
Office of Facilities Engineering and Operations
Security Incident Reporting**

I. System Identification

1. System Name: Security Incident Reporting System
2. Mission Owner: Clair Gill, Director OFEO
3. System Owner: Deron Burba, OCIO Director or Modernization
4. Project Manager: Michelle Gooch and Dan Boyle
5. System Sensitivity: Moderate
6. Date: October 2009
7. Brief (one paragraph) description of the system:

The Security Incident Reporting system provides each major Smithsonian Unit with the ability to track the location, time, and a brief synopsis of any security incidents that occur at a Smithsonian facility. The system also tracks security information for administrative activities and reporting.

II. Privacy Assessment

1. What information is being (or will be) collected.

The Smithsonian security officers are required to collect the names, addresses and phone numbers of any visitor that reports a security incident and any SI staff that might be associated with the incident. The information is collected by the officers and then entered into the Security Incident Report. Generally sensitive personally identifiable information (PII) information (Social Security Numbers, credit card numbers, drivers license numbers), are not recorded. If a visitor at a Smithsonian facility is arrested, additional information will be collected. An arrest report may be scanned into the system and could include: Social Security Number, Place of Birth, Drivers License Number and Arrest Report Number.

2. Why the information is being collected.

This information is used to complete the Office of Protection Services Case Reports and to collect and maintain statistics of various crimes, incidents, or visitor accidents. Contact is made when a visitor is a victim/witness of a crime, incident or is injured while at a Smithsonian facility or property. Case Reports are reviewed by supervisors and if necessary follow-up activities are conducted to ensure the information is accurate and complete.

3. The intended use of the information.

Personal information from the public is needed to identify the individual(s) and perform follow-up with the individual. The names and phone numbers are used to contact these individuals for additional information and to complete internal Smithsonian reviews.

4. With whom the information will be shared.

The Security Information System does not directly interface with any other Smithsonian information systems. On occasion a copy of a case report is requested by the visitor who supplied the incident information, and the report is sent directly to the visitor. Information on Security Incidents is electronically communicated to limited number of OFEO supervisory or management staff members to inform them of incidents occurring within Smithsonian facilities. Reports are also distributed to appropriate offices within the Smithsonian including Museum Directors and the Office of the General Counsel. An incident report may also need to be provided to other agencies such as the National Park Police.

5. What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared.

All information provided to the Smithsonian from the public is collected on a voluntary basis. Visitors are interviewed / questioned on the circumstances of the incident and are aware that a written report containing the information they have given will be recorded.

6. How the information will be secured.

The system is only accessible from the internal Smithsonian network by users that have been authenticated with an approved User ID and password. Internal access to data in the system is based on roles and need to know. The application server and database are located behind Smithsonian firewalls and use secure communication methods. System and database back-up are regularly performed. Data is retained within the database indefinitely.