

United States Environmental Protection Agency
Breach of Personally Identifiable Information (PII)
Contractor Responsibilities and Reporting Procedures

I. Introduction and Overview

The Environmental Protection Agency (EPA) has developed the following procedures for contractors when a suspected or known breach of personally identifiable information (PII)¹ has occurred.

II. Reporting Incidents

Pursuant to EPA's Privacy Policy², contractors are responsible for immediately reporting any suspected or known breach of personally identifiable information (PII) as soon as the incident is discovered to the EPA Call Center at 1-866-411-4372. In addition, the contractor shall inform the Contracting Officer and the Contracting Officer Representative immediately thereafter that the Call Center has been notified of a potential breach of PII.

III. The EPA Call Center

The EPA Call Center will perform the initial assessment of the incident to determine if there has been a breach of PII. At a minimum the contractor shall provide the following information when contacting the call center: the type of PII, how and where PII was stored, number of people affected, the individual (s) responsible, who reported it and the date of occurrence. The Call Center will immediately forward the incident report for investigation.

IV. Full Cooperation

The contractor shall cooperate fully, with Agency personnel during the investigation. To the extent applicable, the contractor shall assist in the containment, control and safeguarding of information to prevent the breach from re-occurring.

Failure to take appropriate action upon discovering the breach, take required steps to prevent a breach from occurring, notify the Agency, or cooperate in the investigation may result in disciplinary actions, parallel law enforcement investigations, or litigation.

1 Definitions: **Personally Identifiable Information (PII)** is any information maintained by the Agency, which can be used to distinguish, trace, or identify an individual's identity, including personal information which is linked or linkable to an individual. Legal name is an example of commonly used PII. **Sensitive Personally Identifiable Information** is a subset of PII and includes a person's Social Security numbers, or comparable identification numbers, financial information and medical information. **Breach** is the loss of control, compromise, unauthorized disclosure, acquisition, or access by persons without authorized access or potential access to PII or Privacy Act information, whether physical or electronic.

2 EPA's Privacy Policy is available at <http://epa.gov/privacy/policy/2151/index.htm>