APPENDIX

FEDERAL LAWS AND POLICIES RELATED TO DATA PRIVACY, SECURITY AND PROTECTING PERSONALLY IDENTIFIABLE AND SENSITIVE INFORMATION

- Privacy Act of 1974 (the Privacy Act) – Governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals maintained in systems of records by Federal agencies. The Privacy Act prohibits the disclosure of information from a system of records without the written consent of the individual, unless the disclosure is permissible under one of twelve statutory exceptions. The Privacy Act also provides individuals with a way to seek access to and amendment of their records and establishes various agency record-keeping requirements. The Privacy Act does not generally apply to personally identifiable information collected and maintained by grantees.

- Computer Security Act of 1987 – Passed to improve the security and privacy of sensitive information in Federal computer systems and created a means for establishing minimum acceptable security practices for such systems. It required agencies to identify their computer systems that contained sensitive information, create computer security plans, and provide security training of system users or owners on the systems that house sensitive information. It was repealed by the Federal Information Security Management Act (FISMA).

- FISMA – Enacted as Title III of the E-Government Act of 2002, FISMA required each Federal agency to develop and implement an agency-wide program to safeguard the information and information systems that support the operational assets of the agency, including the assets managed by other agencies or contractors.

- On May 22, 2006, the Office of Management and Budget (OMB) issued M-06-15, *Safeguarding Personally Identifiable Information*. In this memorandum, OMB directed Senior Officials for Privacy to conduct a review of agency policies and processes and to take necessary corrective action to prevent intentional or negligent misuse of, or unauthorized access to, PII.

- On July 12, 2006, OMB issued M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*. In this memorandum, OMB provided updated guidance for reporting of security incidents involving PII.

- On May 10, 2006, Executive Order 13402 established the President's Task Force on Identity Theft. The Task Force was charged with developing a comprehensive strategic plan for steps the Federal government can take to combat identity theft and recommending actions which can be taken by the public and private sectors. On April 23, 2007, the Task Force submitted its report to the President, titled "Combating Identity Theft: A Strategic Plan." This report is available at www.idtheft.gov.

- On May 22, 2007, OMB issued M 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information. In this memorandum, OMB required agencies to implement a PII breach notification policy within 120 days.

- NIST SP 800-122, Guide to Protecting the Confidentiality of PII – Released by NIST in April 2010, this document is a guide to assist Federal agencies in protecting the confidentiality of PII in information systems. The guide explains the importance of protecting the confidentiality of PII in the context of information security and explains its relationship to privacy. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for incidents involving PII.