STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
HOUSE SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES OF THE COMMITTEE OF OVERSIGHT AND GOVERNMENT REFORM

March 11, 2008

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to speak about the use of commercial information resellers by federal agencies, related provisions contained in H.R. 4791, and privacy safeguards on such information.

Safeguarding the privacy of individuals and ensuring the transparent use of personally identifiable information (PII) by federal agencies has been an Administration priority. Through implementing the recommendations of the President's Identity Theft Task Force, Office of Management and Budget (OMB) guidance, diligent execution of the statutory requirements for System of Record Notices (SORNs) and Privacy Impact Assessments (PIAs), and increased agency reporting, the Administration has improved the protection of personally identifiable information and the transparency of federal use of such information.

Protecting Personally Identifiable Information

Building on the work of the President's Identity Theft Task Force, OMB issued Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," in May 2007 to enhance agency PII protections. M-07-16 required the establishment of agency breach notification policies as well as provided a framework for reducing the risk of PII breaches.

M-07-16 required agencies to review their use of Social Security Numbers (SSNs) and to identify instances in which collection or use of the SSN was unnecessary. Within 120 days from the date of the memo, M-07-16 required agencies to establish a plan to eliminate the unnecessary collection and use of SSNs within 18 months. We are partnering with agencies to explore alternatives to agency use of SSNs as a personal identifier in Federal programs. For Federal employees, the Office of Personnel Management (OPM) is leading the effort to develop a policy for employee identifiers to minimize risk of identify theft.

Additionally, M-07-16 included reminders to encrypt all data on mobile computers/devices carrying agency data, unless the Deputy Secretary makes a written determination that the data is not sensitive. This reminder would apply to agency laptops

and other devices which contain personal information. The encryption must meet National Institute of Standards and Technology (NIST) requirements.

In each Agency's Fourth Quarter FY 2007 E-Government scorecard, OMB included language requiring agencies to submit a status update by December 14th as well as a date when each agency would be in full compliance of the M-07-16 requirements.

In response to one of the task force recommendations, OMB and the Department of Homeland Security (DHS) issued a list of ten common risks impeding adequate protection of government information and best practices for avoiding and mitigating those risks. The risks cover a range of areas, such as security and privacy training, contracts and data sharing agreements, and physical security. All of the best practices and important resources are inter-related and complementary, and can be broadly applied when administering agency information security and privacy programs. The publication can be found at the following site: http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf.

Federal Agency Transparency and Key Privacy Measures

Federal agencies have pursued diligent execution of the statutory requirements for SORNs in the Privacy Act and PIAs in the E-Government Act to ensure transparency for agency use and handling of individuals' information. OMB recently released the FY 2007 Report to Congress on Implementation of the Federal Information Security Management Act of 2002 (FISMA), which reports on key measures of agency privacy programs, including SORNs and PIAs.

For example, the Federal goal is for 90 percent of applicable systems to have publicly posted PIAs. In 2007, 84 percent of applicable systems within the 25 large agencies have publicly posted PIAs. While this percentage remains the same as it was in 2006, the substantial increase in the number of systems identified as requiring a PIA from 2006 to 2007 (an increase of more than 500 systems) is indicative of progress despite no overall increase in the percentage of systems with a PIA. In addition to the high rate of applicable systems with publicly posted PIAs, nineteen of 23 agency Inspectors General reported having its agency PIA process as "satisfactory" or better.

For the percentage of applicable systems of records covered by the Privacy Act to have developed, published, and maintained SORNs, the Federal goal is 90 percent. In 2007, the actual performance was 83. Similar to the PIAs, this percentage remains steady from 2006, though the number of systems identified as requiring a SORN increased by more than 700 systems.

The NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," also identifies conducting PIAs as a control agencies should use and be reviewed during the Certification & Accreditation process. As required by 44 U.S.C. § 3543, Federal agencies must adopt and comply with standards

promulgated by NIST, and identify information security protections consistent with these standards.

In OMB Memorandum 08-09, "New FISMA Privacy Reporting Requirements for FY 2008," we outlined increased reporting of key privacy measures for next year's FISMA report that will enhance public confidence in federal agency privacy programs and further drive agency progress.

Commercial Information Reseller Provisions in H.R. 4791

Privacy warrants the Administration's close attention, in part, due to the need to ensure federal agencies are adhering to the enduring principles of the Privacy Act and the E-Government Act in the face of advances in technology that allow for greater collection, analysis, and storage of information by government, industry, and the non-profit sector. Commercial information resellers, commercial entities that collect information from a range of sources and package them into useful products, are a result of these technological advances. In the course of pursuing their missions, agencies may determine it necessary to obtain these products for a variety of reasons, such as verifying beneficiary addresses or law enforcement efforts. Personally identifiable information federal agencies receive from commercial resellers must receive the same Privacy Act and E-Government protections provided to other information obtained by agencies.

H.R. 4791, the proposed "Federal Agency Data Protection Act" contains two provisions amending the E-Government Act of 2002 intended to strengthen privacy practices specifically relating to agency use of commercial information resellers.

Section 8 defines the term "data broker" and requires agencies to conduct a Privacy Impact Assessment when "purchasing or subscribing for a fee to information in identifiable form from a data broker." I will address the bill's definition of "data broker" later in my testimony. Section 9 prohibits agencies from contracts with data brokers for databases primarily with personally identifiable information without a Privacy Impact Assessment of the data broker's database and requires each agency to promulgate regulations on a range of related standards governing the access, analysis, accuracy, timeliness, use, retention, disclosure, redress for adverse consequences, and enforcement mechanisms to prevent unlawful use.

Although we strongly support enhancing privacy protections for personal information obtained by federal agencies, including information from data brokers, we share several concerns expressed across Federal agencies about the effect of this legislation. In testimony provided to this subcommittee and the Subcommittee on Government Management, Organization, and Procurement on February 14th, I shared concerns that covered the entire bill. Today, I will focus on concerns relating to Sections 8 and 9.

We are concerned the commercial information reseller provisions would have negative unintended consequences without resulting in enhanced privacy protections for agency collection, use, and storage of personal information.

Section 8's and Section 9's new PIA requirements are somewhat duplicative, since federal agencies already conduct PIAs for IT systems receiving information shared by data brokers. OMB guidance on conducing PIAs, M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," directs agencies to conduct a PIA when systematically incorporating identifiable information from commercial sources into its information systems.

For the Section 9 PIA requirement, conducting PIAs on data brokers' propriety systems is legally problematic and could seriously discourage data brokers from offering their services to assist federal agencies. Data brokers could charge agencies substantially higher fees for the increased invasiveness without adding new transparency into how agencies handle personal information, which is already reflected in current PIAs. The applicability of the National Security System exemptions in the E-Government Act to the new requirements is also unclear.

Section 9 also would require specific regulations for agencies to promulgate for contracting with data brokers. Such regulatory rigidity would make it difficult for agencies to adapt to changing realities. Over time, this could leave both agencies and data brokers unable to employ the most effective privacy policies and practices.

Section 8 also broadly defines a "data broker" as "a business entity that, for monetary fees … regularly engages in the practice of collecting, transmitting, or providing access to sensitive information in identifiable form on more than 5,000 individuals who are not the customers or employees of that business entity or affiliate primarily for the purposes of providing such information to non-affiliated third parties on an interstate basis.'' This definition could cover a range of widely used research and reference services as well as routine services, such as change-of-address notification.

We look forward to working with you to ensure that federal agencies privacy policies effectively provide the Privacy Act and E-Government protections for information agencies obtain from commercial resellers, while allowing each agency the ability to maintain privacy policies that align with the ways agencies use and handle the data to pursue their diverse missions.