Subtitle C of title XVI is amended by adding at the end the following new section:

1 SEC. 1622. PRIVACY BREACH REQUIREMENTS.

(a) INFORMATION SECURITY.—

(1) AMENDMENT.—Subchapter III of chapter 35 of title 44, United States Code, is amended by adding at the end the following:

“§ 3550. Privacy breach requirements

“(a) POLICIES AND PROCEDURES.—The Director of the Office of Management and Budget shall establish and oversee policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information, including requirements for—

“(1) not later than 72 hours after the agency discovers such a breach, or discovers evidence that reasonably indicates such a breach has occurred, notice to the individuals whose personally identifiable information could be compromised as a result of such breach;
“(2) timely reporting to a Federal cybersecurity center, as designated by the Director of the Office of Management and Budget; and

“(3) any additional actions that the Director finds necessary and appropriate, including data breach analysis, fraud resolution services, identity theft insurance, and credit protection or monitoring services.

“(b) REQUIRED AGENCY ACTION.—The head of each agency shall ensure that actions taken in response to a breach of information security involving the disclosure of personally identifiable information under the authority or control of the agency comply with policies and procedures established by the Director of the Office of Management and Budget under subsection (a).

“(c) REPORT.—Not later than March 1 of each year, the Director of the Office of Management and Budget shall report to Congress on agency compliance with the policies and procedures established under subsection (a).

“(d) FEDERAL CYBERSECURITY CENTER DEFINED.—The term ‘Federal cybersecurity center’ means any of the following:

“(1) The Department of Defense Cyber Crime Center.
“(2) The Intelligence Community Incident Response Center.

“(3) The United States Cyber Command Joint Operations Center.


“(5) Central Security Service Threat Operations Center of the National Security Agency.

“(6) The United States Computer Emergency Readiness Team.

“(7) Any successor to a center, team, or task force described in paragraphs (1) through (6).

“(8) Any center that the Director of the Office of Management and Budget determines is appropriate to carry out the requirements of this section.”.

(2) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for subchapter III of chapter 35 of title 44, United States Code, is amended by adding at the end the following:

“3550. Privacy breach requirements.”.

(b) Amendments to the E-Government Act of 2002.—Section 208(b)(1)(A) of the E-Government Act of 2002 (44 U.S.C. 3501 note; Public Law 107–347) is amended—

(1) in clause (i), by striking “or” at the end;
(2) in clause (ii), by striking the period at the end and inserting “; or”; and

(3) by adding at the end the following new clause:

“(iii) using information in an identifiable form purchased, or subscribed to for a fee, from a commercial data source.”.

(c) Authority of the Director of the Office of Management and Budget With Respect to Federal Information Policy.—Section 3504(g) of title 44, United States Code, is amended—

(1) in paragraph (1), by striking “and” at the end;

(2) in paragraph (2), by striking “. and” and inserting “; and”; and

(3) by adding at the end the following new paragraph:

“(3) designate a Federal Chief Privacy Officer within the Office of Management and Budget who is a noncareer appointee in a Senior Executive Service position and who is a trained and experienced privacy professional to carry out the responsibilities of the Director with regard to privacy.”.