

(From the E-government Act of 2002 , Pub.L.107-347)

SEC. 208. PRIVACY PROVISIONS. 23

(a) PURPOSE.—The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

(b) PRIVACY IMPACT ASSESSMENTS.

(1) RESPONSIBILITIES OF AGENCIES.

(A) IN GENERAL.—An agency shall take actions described under subparagraph (B) before—

(i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or

(ii) initiating a new collection of information that will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical re-orting requirements imposed on 22 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

(B) AGENCY ACTIVITIES.—To the extent required under subparagraph (A), each agency shall (i) conduct a privacy impact assessment; (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

(C) SENSITIVE INFORMATION.—Subparagraph (B) (iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.

(D) COPY TO DIRECTOR.—Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

(2) CONTENTS OF A PRIVACY IMPACT ASSESSMENT.

(A) IN GENERAL.—The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.

(B) GUIDANCE.—The guidance shall (i) ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and (ii) require that a privacy impact assessment address (I) what information is to be collected; (II) why the information is being collected; (III) the intended use of the agency of the information; (IV) with whom the information will be shared; (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; (VI) how the information will be secured; and (VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the “Privacy Act”).

(3) RESPONSIBILITIES OF THE DIRECTOR.

The Director shall (A) develop policies and guidelines for 13 agencies on the conduct of privacy impact assessments; (B) oversee the implementation of the privacy impact assessment process throughout the Government; and (C) require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

(c) PRIVACY PROTECTIONS ON AGENCY WEBSITES.

(1) PRIVACY POLICIES ON WEBSITES.—

(A) GUIDELINES FOR NOTICES.—The Director shall develop guidance for privacy notices on agency websites used by the public.

(B) CONTENTS.—The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—

- (i) what information is to be collected;
- (ii) why the information is being collected;

- (iii) the intended use of the agency of the information;
- (iv) with whom the information will be shared;
- (v) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
- (vi) how the information will be secured; and
- (vii) the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the ‘Privacy Act’), and other laws relevant to the protection of the privacy of an individual.

(2) PRIVACY POLICIES IN MACHINE-READABLE FORMATS.—The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

(d) DEFINITION.—In this section, the term “identifiable form” means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.