AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Chapter 4[3], provides additional guidance regarding For Official Use Only information.

(c) Do not disclose personal information to anyone outside DoD unless specifically authorized by the Privacy Act (see § 806b.47).

(d) Do not send Privacy Act information to distribution lists or group e-mail addresses unless each member has an official need to know the personal information. When in doubt, send only to individual accounts.

(e) Before forwarding e-mails you have received that contain personal information, verify that your intended recipients are authorized to receive the information under the Privacy Act (see § 806b.47).

Subpart H—Privacy Impact Assessments

§ 806b.30 Evaluating information systems for Privacy Act compliance.

Information system owners and developers must address Privacy Act requirements in the development stage of the system and integrate privacy protections into the development life cycle of the information system. This is accomplished with a Privacy Impact Assessment.

(a) The Privacy Impact Assessment addresses what information is to be collected; why the information is being collected; the intended use of the information; with whom the information will be shared; what notice or opportunities for the individual to decline or consent to providing the information collected, and how that information is shared; secured; and whether a system of records is being created, or an existing system is being amended. The E-Government Act of 2002[4] requires Privacy Impact Assessments to be conducted before:

(1) Developing or procuring information technology systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public.

(2) Initiating a new electronic collection of information in identifiable form for 10 or more persons excluding agencies, instrumentalities, or employees of the Federal Government.

(b) In general, Privacy Impact Assessments are required to be performed and updated as necessary where a system change creates new privacy risks.

(c) No Privacy Impact Assessment is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a Privacy Impact Assessment, or where privacy issues are unchanged.

(d) The depth and content of the Privacy Impact Assessment should be appropriate for the nature of the information to be collected and the size and complexity of the information technology system.

(e) The system owner will conduct a Privacy Impact Assessment as outlined in appendix E to this part and send it to their Major Command Privacy Act office for review and final approval by the Major Command or Headquarters Air Force Functional Chief Information Officer. The Major Command or Headquarters Air Force Functional Chief Information Officer will send a copy of approved Privacy Impact Assessments to Air Force Chief Information Officer/P, 1155 Air Force Pentagon, Washington DC 20330–1155; or e-mail *af.foia@pentagon.af.mil*.

(f) Whenever practicable, approved Privacy Impact Assessments will be posted to the Freedom of Information Act/Privacy Act Web site for public access at *http://www.foia.af.mil* (this requirement will be waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment).

Subpart I—Preparing and Publishing System Notices for the Federal Register

§ 806b.31 Publishing system notices.

The Air Force must publish notices in the FEDERAL REGISTER of new, changed, and deleted systems to inform the public of what records the Air Force keeps and give them an opportunity to comment before the system

[3] *http://www.dtic.mil/whs/directives/corres/pdf/54007r__0998/p54007r.pdf*.

[4] *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107__cong__public__laws&docid=f:publ347.107.pdf*.