or counteract the anticompetitive effects of the acquisition. Developing and obtaining FDA approval for the manufacture and sale of each of the relevant products takes at least 2 years due to substantial regulatory, technological, and intellectual property barriers. In addition to regulatory barriers, penetrating the organ preservation solution market is further hindered by the reluctance of transplant surgeons to switch to a new organ preservation product.

IV. Effects of the Acquisition

The proposed acquisition would cause significant competitive harm to consumers in the U.S. markets for generic trazodone, generic triamterene/HCTZ, and organ preservation solutions by eliminating actual, direct, and substantial competition between Barr and Pliva, by increasing the likelihood that Barr will be able to unilaterally exercise market power, by increasing the likelihood and degree of coordinated interaction between the few remaining competitors, and by increasing the likelihood that consumers will pay higher prices. In these markets, the evidence shows that consumers have obtained lower prices due to the competitive rivalry that exists between market participants. The evidence also shows that as new rivals have entered the markets, consumers have obtained lower prices. The acquisition would also cause significant competitive harm to consumers in the U.S. market for generic nimodipine by eliminating future competition between Barr and Pliva.

V. The Consent Agreement

The proposed Consent Agreement preserves competition in the generic trazodone and triamterene/HCTZ markets by requiring that Barr divest all of the Barr assets for these two products to Apotex within 10 days after the acquisition. The proposed Consent Agreement contains several provisions designed to ensure these divestitures are successful. Barr must provide various transitional services to enable Apotex to compete against Barr immediately following the divestiture. These services include providing Apotex with existing inventory of generic trazodone and triamterene/HCTZ, supplying Apotex with generic trazodone and triamterene/HCTZ until Apotex secures FDA approval to manufacture the products for itself in its own facility, and providing Apotex with all technical assistance necessary to obtain any FDA approvals. Apotex is a reputable generic manufacturer and is well-positioned to manufacture and market the acquired products and to compete effectively in those markets. In the United States, Apotex is roughly the tenth-largest generic pharmaceutical company with over 50 products. Moreover, the acquisition by Apotex does not present competitive problems in either the generic trazodone market or the generic triamterene/HCTZ market because it does not currently compete in those markets.

The proposed Consent Agreement preserves the actual and potential competition in the generic nimodipine market by requiring Barr to divest the Pliva nimodipine assets to Banner no later than 10 days after the acquisition, or to divest its own nimodipine assets to Cardinal no later than 60 days after the acquisition. Banner and Cardinal are both reputable soft-gel capsule manufacturers and particularly well-positioned to manufacture and market generic nimodipine because they are already manufacturing generic nimodipine soft-gel capsules pursuant to their respective joint ventures with Pliva and Barr.

The proposed Consent Agreement preserves the competition in the organ preservation solution market by requiring Barr to divest the Pliva organ preservation solution business to New Custodiol LLC no later than 10 days after the acquisition. The Custodiol product is currently manufactured by a third party, Dr. Franz Kohler Chemie GmbH, who will continue to supply the product to new New Custodiol LLC. New Custodiol LLC is a company that was formed by Pliva's current head of marketing for organ preservation solutions, Mr. Allen Weber, for the purpose of acquiring, marketing and selling Custodiol in the United States. New Custodiol LLC has obtained funding from venture capitalists sufficient to allow it to manufacture and sell Custodiol effectively. The combination of Mr. Allen Weber's industry experience and venture capital backing makes New Custodiol LLC well positioned to acquire Custodiol and to restore the competition that would be lost if the proposed acquisition were to proceed unremedied. If the sale of Pliva's Custodiol is not successful, the Consent Agreement requires that Barr divest its organ preservation solution, ViaSpan, to a Commission-approved acquirer.

If the Commission determines that any of the divestitures or divestees are not acceptable, Barr must rescind the transaction(s) and divest the assets to Commission-approved buyer(s) not later than 6 months from the date the Order becomes final. If Barr fails to divest within the 6 months, the Commission may appoint a trustee to divest the assets.

The proposed remedy also allows for the appointment of an Interim Trustee, experienced in obtaining regulatory approval and the manufacture of pharmaceuticals, to oversee the technology transfer and to assist the divestees in the event of difficulties. As part of the proposed remedy, Barr is required to execute an agreement conferring all rights and powers necessary for the Interim Trustee to satisfy his responsibilities under the Order to assure successful divestitures. The Commission has appointed Mr. William Rahe to be the Interim Monitor and the divestees have consented to his selection. The monitor will ensure that the Commission remains informed about the status of the proposed divestitures and asset transfers.

The purpose of this analysis is to facilitate public comment on the proposed Consent Agreement, and it is not intended to constitute an official interpretation of the proposed Consent Agreement or to modify its terms in any way.

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. E6–17904 Filed 10–24–06; 8:45 am]

BILLING CODE 6750–01–P

GENERAL SERVICES ADMINISTRATION

Privacy Act of 1974; Privacy Act System of Records

AGENCY: General Services Administration

ACTION: Notice of proposed system of records.

SUMMARY: The General Services Administration (GSA) proposes to establish a system of records subject to the Privacy Act of 1974, 5 U.S.C. 552a. This system of records notice is for the GSA Smart Card Program (GSA/CIO–1), which covers the Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD–12), process after adjudication and determines if the individual can receive identification (ID) card. The records include both mandatory and optional information necessary to the request for an ID card, registration, verification, and issuance procedures, the index/database of active and invalid ID cards, and the information stored on the ID cards. The system may include records of individuals who entered and

exited Federal facilities or accessed systems.

The GSA Smart Card Program will ensure the safety and security of Federal facilities, information systems, and their occupants and users, by verifying that all persons entering Federal facilities, using Federal information resources, or accessing classified information are authorized to do so. The system also will track and control identification ID cards issued to individuals for these purposes.

DATE: The system of records will become effective on December 4, 2006 unless comments received on or before that date result in a contrary determination.

ADDRESSES: Comments relating to the GSA Smart Card Program should be directed to: Director, GSA HSPD–12 Smart Card Program Management Office, Office of the Chief Information Officer, General Services Administration, 1800 F Street NW., Room G–006, Washington DC 20405–0002; telephone (202) 501–1500; fax (202) 219–5818.

FOR FURTHER INFORMATION CONTACT: GSA Privacy Act Officer (CIB), General Services Administration, 1800 F Street NW, Washington, DC 20405; telephone (202) 501–1452.

SUPPLEMENTARY INFORMATION: The GSA notice entitled Credentials, Passes, and Licenses (GSA/HRO–8) is cancelled. However, existing GSA forms and associated databases covered by that system will continue in effect until replaced with those covered by this notice. The existing forms include: GSA Form 48, Request and Record of Identification; GSA Form 277, Employee Identification and Authorization Credential; GSA Form 277U, Temporary Pass; GSA Form 277V, Visitor Pass; GSA Form 2941 Parking Application; as well as biometric information including photo, fingerprints and signature. The new forms and databases covered by this notice will be phased in to ensure a controlled and structured process.

Dated: October 6, 2006.

Cheryl M. Paige,

Acting Director, Office of Information Management.

GSA/CIO–1

System name: GSA Smart Card Program

System location: Data are maintained in GSA Central Office databases with access from GSA regional offices. Additionally, some access control data may be located in Federal buildings and Federally-leased facilities where staffed guard stations have been established to handle the GSA Smart Card Personal Identity Verification (PIV) process as well as the physical security and computer security offices at those locations. Contact the System Manager for additional information.

Security classification: Most identity records are not classified. However, in some cases, records of certain individuals or portions of some records may be classified in the interest of national security.

Categories of individuals covered by the system: Individuals who require regular, ongoing access to agency facilities, information technology systems, or information classified in the interest of national security, including:

a. Applicants for employment or contracts

b. Federal employees

c. Contractors

d. Students

e. Interns

f. Volunteers

g. Individuals formerly in any of these positions

Also included are individuals authorized to perform or use services provided in agency facilities (*e.g.*, Credit Union, Fitness Center, Cafeteria, etc.).

The system does not apply to occasional visitors or short-term guests, to whom GSA will issue temporary identification and credentials.

Categories of records in the system:

a. Records maintained on individuals issued credentials by GSA include the following data fields:

- Full name,
- Social Security Number (SSN)
- Date of birth
- Signature
- Image (photograph)
- Fingerprints
- Hair color
- Eye color
- Height
- Organization / office of assignment
- Company / agency name
- Telephone number
- ID card issuance and expiration dates
- ID card request form
- Registrar approval signature
- ID card number
- Emergency responder designation
- Copies of documents used to verify identification or information derived from those documents such as document title, document issuing authority, document number, document expiration date, other document information

b. Records maintained on cardholders entering GSA facilities or using GSA systems may include:

- Name
- ID card number
- Date and Time of entry/exit
- Location of entry and exit
- Computer access dates, times, and locations

Authorities for maintenance of the system:

a. 5 U.S.C. 301;

b. Federal Information Security Management Act (Pub. L. 107–296);

c. E-Government Act (Pub. L. 107–347, Sec. 203);

d. Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.)

e. Government Paperwork Elimination Act (Pub. L. 105–277, 44 U.S.C. 3504);

f. Homeland Security Presidential Directive 12 (HSPD–12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; and

g. Federal Property and Administrative Services Act of 1949, as amended.

Purpose: The primary purposes of the system are:

a. To ensure the safety and security of GSA facilities, systems or information, and our occupants and users;

b. To verify that all persons entering federal facilities, using federal information resources, or accessing classified information are authorized to do so; and

c. To track and control ID cards issued to persons entering and exiting the facilities, using systems, or accessing classified information.

Routine uses of the system records, including categories of users and their purpose for using the system:

Information about covered individuals may be disclosed without consent as permitted by the Privacy Act of 1974, 5 U.S.C. § 552a(b), and:

a. To the Department of Justice when: (1) GSA or any component thereof; (2) any employee of GSA in his or her official capacity; (3) any employee of GSA in his or her individual capacity where GSA or the Department of Justice (DOJ) has agreed to represent the employee; or (4) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, GSA determines that the records are both relevant and necessary to the litigation, and the use of such records by DOJ is therefore deemed by GSA to be for a purpose compatible with the purpose for which GSA collected the records.

b. To a court or adjudicative body in a proceeding when: (1) GSA or any component thereof; (2) any employee of GSA in his or her official capacity; (3) any employee of GSA in his or her

individual capacity where GSA or the Department of Justice has agreed to represent the employee; or (4) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, GSA determines that the records are both relevant and necessary to the litigation, and the use of such records is therefore deemed by GSA to be for a purpose that is compatible with the purpose for which the agency collected the records.

c. Except as noted on Forms SF 85, 85–P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.

d. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent whose record is maintained.

e. To the National Archives and Records Administration for records management purposes.

f. To agency contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

g. To a Federal, State, local, foreign, tribal, or other public authority the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action.

h. To the Office of Management and Budget when necessary to the review of private relief legislation pursuant to OMB Circular No. A-19.

i. To a Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives.

j. To notify another federal agency when, or verify whether, an ID card is no longer valid.

Note: Disclosures within GSA of data pertaining to date and time of entry and exit of an agency employee working in the District of Columbia may not be made to supervisors, managers or any other persons (other than the individual to whom the information applies) to verify employee time and attendance record for personnel actions because 5 U.S.C. § 6106 prohibits Federal executive agencies (other than the Bureau of Engraving and Printing) from using a recording clock within the District of Columbia, unless used as a part of a flexible schedule program under 5 U.S.C. § 6120 *et seq.*

Policies and practices for storing, retrieving, accessing, retaining, and disposing of system records:

Storage: Information may be collected on paper or electronically and may be stored on paper or on electronic media, as appropriate.

Retrievability: Records are retrievable by name, Social Security Number, other ID number, ID card number, image (photograph), and fingerprint.

Safeguards: Paper records are kept in locked cabinets in secure facilities and access to them is restricted to individuals whose role requires use of the records.

The computer servers in which records are stored are located in facilities that are secured by alarm systems and off-master key access. The computer servers themselves are password-protected. Access to individuals working at guard stations is password-protected; each person granted access by the system at guard stations must be individually authorized to use the system. A Privacy Act Warning Notice appears on the monitor screen when records containing information on individuals are first displayed. Data exchanged between the servers and the client PCs at the guard stations and badging office are encrypted. Backup tapes are stored in a locked and controlled room in a secure, off-site location. Each of the component computer servers at the GSA Regions, or at the contract Card Production and Card Management Systems has been only authorized to act when it has been Certified and Accredited in accord with GSA Information Technology Security Policy and HSPD–12 criteria. This Certification is updated periodically on a 3 year basis, or less if cause to do so has become apparent.

An audit trail is maintained and reviewed periodically to identify unauthorized access. Persons given roles in the personal identity verification process must complete training specific to their roles to ensure they are knowledgeable about how to protect individually identifiable information.

Retention and disposal: Records relating to persons covered by this system are retained in accordance with General Records Schedule 18, Item 17. Unless retained for specific, ongoing security investigations for maximum security facilities, records of access are maintained for five years and then destroyed by degaussing hard drives and shredding paper. For other facilities, records are maintained for two years and then destroyed by wiping hard drives and shredding paper. All other records relating to employees are destroyed two years after the ID card expiration date.

In accordance with HSPD–12, ID cards are deactivated within 18 hours of cardholder separation, loss of card, or expiration. The information on ID cards is maintained in accordance with General Records Schedule 11, Item 4. ID cards are destroyed by shredding 90 days after deactivation. Once notification of deactivation has been received, the ID number is placed on a revocation list within no more than 2 hours, which immediately invalidates the access privileges for that card in accord with GSA policy.

System manager and address:

Director, GSA HSPD–12 Smart Card Program Management Office

Office of the Chief Information Officer

1800 F Street NW, Room G–006

Washington DC 20405–0002

Notification procedure: An individual can determine if this system contains a record pertaining to him/her by sending a request in writing, signed, to the System Manager at the above address.

When requesting notification of or access to records covered by this notice, an individual should provide his/her full name, date of birth, agency name, and work location. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to access, such as a government-issued photo ID.

Record access procedures: Same as notification procedures. Requesters also should reasonably specify the record contents being sought. Rules regarding access to Privacy Act records appear in 41 CFR part 105–64. If additional information or assistance is required, contact the GSA Privacy Act Officer (CIB), General Services Administration, 1800 F Street NW, Washington, DC 20405; telephone (202) 501–1452.

Contesting record procedures: Same as notification procedures. Requesters also should reasonably identify the record, specify the information they are contesting, state the corrective action sought and the reasons for the correction, along with supporting justification showing why the record is not accurate, timely, relevant, or complete. Rules regarding amendment of Privacy Act records appear in 41 CFR part 105–64. If additional information or assistance is required, contact the GSA Privacy Act Officer.

Record source categories: Employee, contractor, or applicant; sponsoring agency; former sponsoring agency; other Federal agencies; contract employer; former employer.

Exemptions claimed for the system: None.

[FR Doc. E6–17896 Filed 10–24–06; 8:45 am]

BILLING CODE 6820–34–S

OFFICE OF GOVERNMENT ETHICS

No FEAR Act Notice

AGENCY: Office of Government Ethics (OGE).

ACTION: Notice.

SUMMARY: The Office of Government Ethics is publishing this notice under the ''Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002,'' which is known as the No FEAR Act, to inform current employees, former employees, and applicants for OGE employment of the rights and protections available to them under Federal antidiscrimination, whistleblower protection and retaliation laws.

FOR FURTHER INFORMATION CONTACT: Vincent J. Salamone, Associate General Counsel, Office of General Counsel and Legal Policy, Office of Government Ethics, Suite 500, 1201 New York Avenue, NW., Washington, DC 20005–3917; OGE Internet E-mail: *usoge@oge.gov* (for E-mail messages, the subject line should include the following reference—''No FEAR Act Notice''); Telephone: 202–482–9274; TDD: 202–482–9293; FAX: 202–482–9237. A copy of the No FEAR Act Notice will be posted on OGE's Web site (*http://www.usoge.gov*). Persons who cannot access this No FEAR Act notice through the Internet may request a paper or electronic copy by contacting Mr. Salamone at the address, E-mail address, telephone numbers, or FAX number listed above.

SUPPLEMENTARY INFORMATION: On May 15, 2002, Congress enacted the ''Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002,'' which is now known as the No FEAR Act. One purpose of the Act is to require that Federal agencies be accountable for violations of antidiscrimination and whistleblower protection laws. In support of this purpose, Congress found that ''agencies cannot be run effectively if those agencies practice or tolerate discrimination.'' Public Law 107–174, Section 101(1), 116 Stat. 566. The Act also requires this Agency to provide this notice to Federal employees, former Federal employees and applicants for Federal employment to inform them of the rights and protections available to them under Federal antidiscrimination, whistleblower protection, and retaliation laws.

Antidiscrimination Laws

A Federal agency cannot discriminate against an employee or applicant with respect to the terms, conditions or privileges of employment on the basis of race, color, religion, sex, national origin, age, disability, marital status or political affiliation. Discrimination on these bases is prohibited by one or more of the following statutes: 5 U.S.C. 2302(b)(1), 29 U.S.C. 206(d), 29 U.S.C. 631, 29 U.S.C. 633a, 29 U.S.C. 791 and 42 U.S.C. 2000e–16.

If you believe that you have been the victim of unlawful discrimination on the basis of race, color, religion, sex, national origin or disability, you must contact an Equal Employment Opportunity (EEO) counselor within 45 calendar days of the alleged discriminatory action, or, in the case of a personnel action, within 45 calendar days of the effective date of the action, before you can file a formal complaint of discrimination with your agency. *See, e.g.*, 29 CFR part 1614. If you believe that you have been the victim of unlawful discrimination on the basis of age, you must either contact an EEO counselor as noted above or give notice of intent to sue to the Equal Employment Opportunity Commission (EEOC) within 180 calendar days of the alleged discriminatory action. If you are alleging discrimination based on marital status or political affiliation, you may file a written complaint with the U.S. Office of Special Counsel (OSC) at 1730 M Street, NW., Suite 218, Washington, DC 20036–4505 or online through the OSC Web site—*http://www.osc.gov.* In the alternative (or in some cases, in addition), you may pursue a discrimination complaint by filing a grievance through your agency's administrative or negotiated grievance procedures, if such procedures apply and are available.

Whistleblower Protection Laws

A Federal employee with authority to take, direct others to take, recommend or approve any personnel action must not use that authority to take or fail to take, or threaten to take or fail to take, a personnel action against an employee or applicant because of disclosure of information by that individual that is reasonably believed to evidence violations of law, rule or regulation; gross mismanagement; gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety, unless disclosure of such information is specifically prohibited by law and such information is specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs.

Retaliation against an employee or applicant for making a protected disclosure is prohibited by 5 U.S.C. 2302(b)(8). If you believe that you have been the victim of whistleblower retaliation, you may file a written complaint (Form OSC–11) with OSC at 1730 M Street, NW., Suite 218, Washington, DC 20036–4505 or online through the OSC Web site—*http://www.osc.gov.*

Retaliation for Engaging in Protected Activity

A Federal agency cannot retaliate against an employee or applicant because that individual exercises his or her rights under any of the Federal antidiscrimination or whistleblower protection laws listed above. If you believe that you are the victim of retaliation for engaging in protected activity, you must follow, as appropriate, the procedures described in