procedures that protect the confidentiality, security, and integrity of personal information collected from children; and

(5) the Rule requires operators to provide reasonable means for the parent to review the information.

The FTC staff retains its estimate that roughly 30 new web entrants each year will fall within the Rule's coverage and that, on average, new entrants will spend approximately 60 hours crafting a privacy policy, designing mechanisms to provide the required online privacy notice and, where applicable, the direct notice to parents.[3] Accordingly, staff estimates that complying with the Rule's disclosure requirements will require approximately 1,800 hours (30 new web entrants x 60 hours per entrant). Consistent with prior estimates, FTC staff estimates that the time spent on compliance would be apportioned five to one between legal (lawyers or similar professionals) and technical (computer programmers) personnel. Staff therefore estimates that lawyers or similar professionals who craft privacy policies will account for 1,500 of the 1,800 hours required. Computer programmers responsible for posting privacy policies and implementing direct notices and parental consent mechanisms will account for the remaining 300 hours.

Website operators that have previously created or adjusted their sites to comply with the Rule will incur no further burden associated with the Rule, unless they opt to change their policies and information collection in ways that will further invoke the Rule's provisions. Moreover, staff believes that existing COPPA-compliant operators who introduce additional sites beyond those they already have created will incur minimal, if any, incremental PRA burden. This is because such operators already have been through the start-up phase and can carry over the results of that to the new sites they create.

(b) *Reporting Requirements for Safe Harbor Applicants:* 100 hours

Operators can comply with the Rule by meeting the terms of industry self-regulatory guidelines that the Commission approves after notice and comment.[4] While the submission of industry self-regulatory guidelines to the agency is voluntary, the Rule includes specific reporting requirements that all safe harbor applicants must provide to receive Commission approval. Staff retains its estimate that it would require, on average, 265 hours per new safe harbor program applicant to prepare and submit its safe harbor proposal in accordance with Section 312.10(c) of the Rule. Industry sources have confirmed that this estimate is reasonable and advised that all of this time would be attributable to the efforts of lawyers. Given that several safe harbor programs are already available to website operators, FTC staff believes that it is unlikely that more than one additional safe harbor applicant will submit a request within the next three years of PRA clearance sought. Thus, annualized burden attributable to this requirement would be approximately 85 hours per year (265 hours ÷ 3 years) or, roughly, 100 hours. Staff believes that most of the records submitted with a safe harbor request would be those that these entities have kept in the ordinary course of business, and that any incremental effort associated with maintaining the results of independent assessments or other records under Section 312.10(d)(3) also would be in the normal course of business. In accordance with the regulations implementing the PRA, the burden estimate excludes effort expended for these activities. 5 CFR 1320.3(b)(2).

Accordingly, FTC staff estimates that total burden per year for disclosure requirements affecting new web entrants and reporting requirements for safe harbor applications would be approximately 2,000 hours, rounded to the nearest thousand.

Labor costs: Labor costs are derived by applying appropriate hourly cost figures to the burden hours described above. Staff conservatively assumes hourly rates of $150 and $35, respectively, for lawyers or similar professionals and computer programmers.[5] Based on these inputs, staff further estimates that associated annual labor costs for new entrants would be $235,000 [(1,500 hours x $150 per hour for legal) + (300 hours x $35 per hour for computer programmers)] and $15,000 for safe harbor applicants (100 hours per year x $150 per hour), for a total labor cost of $250,000.

Non-labor costs: Because websites will already be equipped with the computer equipment and software necessary to comply with the Rule's notice requirements, the sole costs incurred by the websites are the aforementioned estimated labor costs. Similarly, industry members should already have in place the means to retain and store the records that must be kept under the Rule's safe harbor recordkeeping provisions, because they are likely to have been keeping these records independent of the Rule.

David C. Shonka,

Acting General Counsel.

[FR Doc. E8–14148 Filed 6–23–08: 8:45 am]

BILLING CODE 6750–01–S

[3] Although staff cannot determine with any degree of certainty the number of new entrants potentially subject to the Rule, it believes its estimate is reasonable. The Commission received no comments challenging staff's prior PRA analyses in its prior requests for renewed clearance for the Rule or when it most recently sought comment on the Rule itself (70 FR 21107, 21109, April 22, 2005). Accordingly, staff retains those estimates for the instant PRA analysis. For the same reasons, staff retains its prior estimate of 60 hours per new entrant.

[4] *See* Section 312.10(c). Approved self-regulatory guidelines can be found on the FTC's website at (*http://www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html.*)

[5] FTC staff estimates average legal costs at $150 per hour, which is roughly midway between Bureau of Labor Statistics (BLS) mean hourly wages shown for attorneys (approximately $55) in the most recent whole-year data available online (2006) and what staff believes may more generally reflect hourly attorney costs ($250) associated with Commission information collection activities. The $35 estimate for computer programmers is also conservatively based on the most recent whole-year data available online from the BLS (2006 National Compensation Survey and 2006 Occupational Employment and Wage Statistics).

GENERAL SERVICES ADMINISTRATION

Privacy Act of 1974; Notice of Updated Systems of Records

AGENCY: General Services Administration.

ACTION: Notice.

SUMMARY: GSA reviewed its Privacy Act systems to ensure that they are relevant, necessary, accurate, up-to-date, covered by the appropriate legal or regulatory authority, and compliant with OMB M–07–16. This notice is an updated Privacy Act system of records notice.

DATES: Effective July 24, 2008.

FOR FURTHER INFORMATION CONTACT: Call or e-mail the GSA Privacy Act Officer: telephone 202–208–1317; e-mail *gsa.privacyact@gsa.gov*.

ADDRESSES: GSA Privacy Act Officer (CIB), General Services Administration, 1800 F Street, NW., Washington, DC 20405.

SUPPLEMENTARY INFORMATION: GSA undertook and completed an agency-wide review of its Privacy Act systems of records. As a result of the review, GSA is publishing an updated Privacy Act system of records notice. The revised system notice clarifies the authorities and practices regarding the collection and maintenance of information, but does not change individuals' rights to access or amend their records in the system of records. The updated system notice also

includes the new requirement from OMB Memorandum M–07–16 regarding a new routine use that allows agencies to disclose information in connection with a response and remedial efforts in the event of a data breach.

Dated: June 12, 2008.

Cheryl M. Paige,

Director, Office of Information Management.

GSA/CIO–1

SYSTEM NAME:

Enterprise Level Identity Verification System (ELIVS).

SYSTEM LOCATION:

ELIVS comprises a Web based application and data is maintained in a secure server facility at GSA Central Office, located at 1800 F Street, NW., Washington, DC 20405. Additionally, some fingerprint data may be located in GSA facilities where staffed fingerprint collection stations (Live Scan system) have been established to handle the contractor Personal Identity Verification (PIV) process. Contact the System Manager for additional information.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who require routine access to agency facilities and information technology systems, including:

a. Federal employees.

b. Contractors.

c. Child care workers and other temporary workers with similar access requirements.

The system does not apply to occasional visitors or short-term guests, to whom GSA facilities may issue local Facility Access Cards (FAC).

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains information needed for issuing and maintaining HSPD–12 credentials and also access privilege information. Records may include:

- Employee/contractor/other worker full name
- Social Security Number (SSN)
- Date of birth
- Facial Image
- Fingerprints (within the Live Scan systems)
- Organization/office of assignment
- Company/agency name
- Telephone number
- ID card issuance and expiration dates
- ID card number
- Emergency responder designation
- Home address and work location
- Contract and supervisor information

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301, 40 U.S.C. 121, 40 U.S.C. 582, 40 U.S.C. 3101, 44 U.S.C. 3501, 44 U.S.C. 3506, 44 U.S.C. 3602, E.O. 9397, and Homeland Security Presidential Directive 12 (HSPD–12).

PURPOSE:

The primary purposes of the system are:

To act as an authoritative source for GSA identities including employees, contractors, and other workers to verify that all persons requiring routine access to GSA facilities or using GSA information resources have sufficient background investigations and are permitted access, to track and manage HSPD–12 ID cards issued to persons who have routine access to GSA facilities and information systems, and to provide reports of identity data for administrative and staff offices to efficiently track and manage contractors.

ROUTINE USES OF THE SYSTEM RECORDS, INCLUDING CATEGORIES OF USERS AND THEIR PURPOSE FOR USING THE SYSTEM:

System information may be accessed and used by:

a. GSA Personnel when needed for official business, including the Security Office, HSPD–12 Points of Contacts, and designated analysts and managers for official business; PIV card requesting officials and Human Resource Officers to track, verify, and update identity information of GSA personnel; and Regional Credential Officers (RCOs) to issue and track PIV ID cards;

b. To verify suitability of an employee or contractor before granting access to specific resources;

c. To disclose information to agency staff and administrative offices who may restructure the data for management purposes;

d. An authoritative source of identities for Active Directory and Lotus Notes and other GSA systems;

e. In any legal proceeding, where pertinent, to which GSA is a party before a court or administrative body;

f. To authorized officials engaged in investigating or settling a grievance, complaint, or appeal filed by an individual who is the subject of the record.

g. To a Federal, state, local, foreign, or tribal agency in connection with the hiring or retention of an employee; the issuance of a security clearance; the reporting of an investigation; the letting of a contract; or the issuance of a grant, license, or other benefit to the extent that the information is relevant and necessary to a decision;

h. To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), or the Government Accountability Office (GAO) when the information is required for program evaluation purposes;

i. To a Member of Congress or staff on behalf of and at the request of the individual who is the subject of the record;

j. To an expert, consultant, or contractor of GSA in the performance of a Federal duty to which the information is relevant;

k. To the National Archives and Records Administration (NARA) for records management purposes;

l. To appropriate agencies, entities, and persons when (1) the Agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by GSA or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING RECORDS IN THE SYSTEM:

STORAGE:

Computer records are stored on a secure server and accessed over the web using encryption software. Paper records, when created, are kept in file folders and cabinets in secure rooms. The Live Scan systems are kept in secure locations with limited access to authorized personnel only.

RETRIEVABILITY:

Records are retrievable by a combination of first name and last name. Group records are retrieved by organizational code.

SAFEGUARDS:

Computer records are protected by a password system. Paper records are stored in locked metal containers or in secured rooms when not in use. Information is released to authorized officials based on their need to know.

RETENTION AND DISPOSAL:

Records are disposed of as specified in the handbook, GSA Records Maintenance and Disposition System (CIO P 1820.1).

SYSTEM MANAGER AND ADDRESS:

Program Manager, HSPD–12 Program Management Office, General Services Administration, 1800 F Street, NW., Room 2208 Washington, DC 20405.

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, region/office, 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.

CONTESTING RECORD PROCEDURES:

Rules for contesting the content of a record and appealing a decision are contained in 41 CFR 105–64.

RECORD SOURCES CATEGORIES:

The sources for information in the system are the individuals about whom the records are maintained, the supervisors of those individuals, existing GSA systems, sponsoring agency, former sponsoring agency, other Federal agencies, contract employer, former employer, and the U.S. Office of Personnel Management (OPM).

[FR Doc. E8–14199 Filed 6–23–08; 8:45 am]

BILLING CODE 6820–34–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Agency for Healthcare Research and Quality

Agency Information Collection Activities: Proposed Collection; Comment Request

AGENCY: Agency for Healthcare Research and Quality, HHS.

ACTION: Notice.

SUMMARY: This notice announces the intention of the Agency for Healthcare Research and Quality (AHRQ) to request that the Office of Management and Budget (OMB) approve the proposed information collection project: ''Assessing the Impact of the Patient Safety Improvement Corps (PSIC) Training Program.'' In accordance with the Paperwork Reduction Act of 1995, 44 U.S.C. 3506(c)(2)(A), AHRQ invites the public to comment on this proposed information collection.

This proposed information collection was previously published in the **Federal Register** on April 16th, 2008 and allowed 60 days for public comment. No comments were received. The purpose of this notice is to allow an additional 30 days for public comment.

DATES: Comments on this notice must be received by July 24, 2008.

ADDRESSES: Written comments should be submitted to: AHRQTs OMB Desk Officer by fax at (202) 395–6974 (attention: AHRQ's desk officer) or by e-mail at *OIRA_submission@omb.eop.gov* (*attention:* AHRQ's desk officer).

Copies of the proposed collection plans, data collection instruments, and specific details on the estimated burden can be obtained from the AHRQ Reports Clearance Officer.

FOR FURTHER INFORMATION CONTACT: Doris Lefkowitz, AHRQ Reports Clearance Officer, (301) 427–1477, or by e-mail at *doris.letkowitz(2iahrg.hhs.gov*.

SUPPLEMENTARY INFORMATION:

Proposed Project

Assessing the Impact of the Patient Safety Improvement Corps (PSIC) Training Program

AHRQ proposes to assess the impact of the PSIC training program. This three-week program was designed and implemented by AHRQ and the Veteran's Administration's (VA) National Center for Patient Safety (NCPS) to improve patient safety by training participants in various patient safety concepts, tools, information, and techniques. The PSIC program represents a new approach to training for AHRQ by focusing on disseminating patient safety information and building skill sets to ultimately foster a national network of individuals who support, promote, and speak a common language of patient safety. Participants have included representatives from State health departments, hospitals and health systems, Quality Improvement Organizations, and a very small number of other types of organizations. AHRQ will use an independent contractor to conduct the assessment of the PSIC training program. The goal of the assessment is to determine the extent to which the PSIC concepts, tools, information, and techniques have been used on the job by training participants and successfully disseminated within and beyond the participating organizations, local areas, regions, and states. AHRQ is assessing the PSIC program pursuant to its authority under 42 U.S.C. 299(b) and 42 U.S.C. 299a(a) to evaluate its strategies for improving health care quality.

The assessment involves two Web-based questionnaires to examine post-training activities and patient safety outcomes of the training from multiple perspectives. One questionnaire is directed to training participants while the other is directed to leaders of the organizations from which the training participants were selected. Questionnaires will focus on the following topics: (1) Post-PSIC activities (including how PSIC material has been utilized in their home organizations, types of patient safety activities conducted post-PSIC, and number of people trained in some or all aspects of PSIC since their attendance); (2) barriers to and facilitators of the use of PSIC in the workplace; and (3) perceived outcomes of PSIC participation (e.g., improved patient safety; improved patient safety processes, standards, or policies; improved investigative and analytical processes and selection and implementation of patient safety interventions; improved patient safety culture; improved communications).

Method of Collection

All training participants and organizational leaders from participating organizations will be invited to respond to their corresponding Web-based questionnaire. Invitations will be sent via e-mail, using contact information previously collected by AHRQ and NCPS. Standard non response follow-up techniques, such as two reminder e-mails that include the link to the questionnaire, will be used. Individuals and organizations will be assured of the privacy of their responses.

Estimated Annual Respondent Burden

Exhibit 1 shows the estimated annualized burden hours for the respondent's time to participate in the study. The training participant questionnaire is estimated to require 30 minutes to complete and the organizational leader questionnaire is estimated to require 15 minutes to complete, resulting in a total burden of 169 hours.