collection of health professions or nursing student loan funds, to locate the defaulted borrower to collect the loan. Any school which requests and obtains this address information must comply with the requirements of HRSA and the IRS regarding the safeguarding and proper handling of this information.

6. To appropriate federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information maintained in this system of records, and the information disclosed is relevant and necessary for that assistance.

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

STORAGE:

Records are maintained in the DMS or in file folders and/or computer data files.

RETRIEVABILITY:

Retrieval of data and case files is by subject's name or institution ID.

SAFEGUARDS:

• Authorized users: Access is limited to authorized HHS staff and contractors in performance of their duties. Authorized personnel include the contractor/system manager and his staff who have responsibilities for administering the programs. HRSA maintains current lists of authorized users. Institutions do not have remote access to this system.

• Physical safeguards: The DMS is housed on an HRSA server behind a firewall. The DMS is an intra-office system only for the sole use of CBB staff. All computer equipment and files and hard copy files are stored in areas where fire and life safety codes are strictly enforced. All automated and non-automated documents are protected on a 24-hour basis. Perimeter security includes intrusion alarms, on-site guard force, random guard patrol, key/passcard/combination controls, and receptionist controlled area. Hard copy files are maintained in a file room used solely for this purpose with access limited by combination lock to authorized users identified above. Computer files are password protected and are accessible only by use of computers which are password protected.

• Procedural safeguards: A password is required to access computer files. All users of personal information in connection with the performance of their jobs protect information from public view and from unauthorized personnel entering an unsupervised area. All passwords, keys and/or combinations are changed when a person leaves or no longer has authorized duties. Access to records is limited to those authorized personnel trained in accordance with the Privacy Act and ADP security procedures. The safeguards described above were established in accordance with DHHS chapter 45–13 and supplementary chapter PHS hf: 45–13 of the General Administration Manual; and the DHHS Information Resources Management Manual, Part 6, "ADP Systems Security."

RETENTION AND DISPOSAL:

HRSA is working with the Records Officer and NARA to obtain the appropriate retention value.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of Student Loans and Scholarships, Bureau of Health Professions, Health Resources and Services Administration, Department of Health and Human Services, 5600 Fishers Lane, Room 9–105, Rockville, Maryland 20857.

NOTIFICATION PROCEDURE:

Requests concerning whether the system contains records about you should be made to the Systems Manager. When requesting notification of or access to records covered by this Notice, an individual must provide his/her full name, date of birth, and other proof of identity as required for Privacy Requests.

• Request in person: A subject individual who appears in person at a specific location seeking access or disclosure of records relating to him/her shall provide his/her name, current address, and at least one piece of tangible identification such as driver's license, passport, voter registration card, or union card. Identification papers with current photographs are preferred but not required. Additional identification may be requested when there is a request for access to records which contain an apparent discrepancy between information contained in the records and that provided by the individual requesting access to the records. Where the subject individual has no identification papers, the responsible agency official shall require that the subject individual certify in writing that he/she is the individual who he/she claims to be and that he/she understands that the knowing and willful request or acquisition of a record concerning an individual under false pretenses is a criminal offense subject to a $5,000 fine.

• Requests by telephone: Because positive identification of the caller cannot be established, no requests by telephone will be honored.

• Requests by mail: A written request must contain the name and address of the requester, and his/her signature which is either notarized to verify his/her identify or includes a written certification that the requester is the person he/she claims to be and that he/she understands that the knowing and willful request or acquisition of records pertaining to an individual under false pretenses is a criminal offense subject to a $5,000 fine.

CONTESTING RECORD PROCEDURES:

Any record subject may contest the accuracy of information on file at CBB by writing to the Director, Division of Student Loans and Scholarships, Bureau of Health Professions, Health Resources and Services Administration, Department of Health and Human Services, 5600 Fishers Lane, Room 9–105, Rockville, Maryland 20857. The request should contain a reasonable description of the record, specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely or irrelevant.

RECORD SOURCE CATEGORIES:

1. Educational institutions participating in CBB programs.

2. Financial aid officers administering CBB programs.

3. Student borrowers and recipients participating in CBB programs.

4. Borrowers submitted for uncollectible debt write-offs.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 2010–2242 Filed 2–2–10; 8:45 am]

BILLING CODE 4160–15–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2010–0004]

National Protection and Programs Directorate; Communications Unit Leader (COML) Prerequisite and Evaluation

AGENCY: National Protection and Programs Directorate, Department of Homeland Security.

ACTION: 60-Day Notice and request for comments; New Information Collection Request: 1670–NEW.

SUMMARY: The Department of Homeland Security, National Protection and Programs Directorate/Cybersecurity and Communications/Office of Emergency Communications (OEC), has submitted the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995 (Pub. L. 104–13, 44 U.S.C. Chapter 35).

DATES: Comments are encouraged and will be accepted until April 5, 2010. This process is conducted in accordance with 5 CFR 1320.1.

ADDRESSES: Written comments and questions about this Information Collection Request should be forwarded to OEC, Attn.: Jonathan Clinton, *Jonathan.Clinton@dhs.gov.* Written comments should reach the contact person listed no later than April 5, 2010. Comments must be identified by DHS–2010–0004 and may be submitted by *one* of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.*
- *E-mail: Jonathan.Clinton@dhs.gov.*

Include the docket number in the subject line of the message.

Instructions: All submissions received must include the words "Department of Homeland Security" and the docket number for this action. Comments received will be posted without alteration at *http://www.regulations.gov,* including any personal information provided.

SUPPLEMENTARY INFORMATION: OEC, formed under Title XVIII of the Homeland Security Act of 2002, 6 U.S.C. 101 *et seq.,* as amended, is responsible for conducting nationwide outreach and providing technical assistance to foster the development of interoperable emergency communications capabilities for State, regional, local, and tribal governments. OEC is addressing these responsibilities, in part, by offering an All Hazards Type III COML training course for State, regional, and local emergency response stakeholders. Participation in these courses requires satisfaction of several prerequisites, the completion of which will be verified using a certification form. In addition, to evaluate course delivery for quality assurance and improvement purposes, evaluation data will be collected in an evaluation form. OEC will use this information to identify course attendees, verify satisfaction of course prerequisites, and evaluate course delivery for quality and improvement purposes. The collection of information is mostly electronic but can also be received in paper form to facilitate ease of registration and evaluation of OEC events. Evaluation forms will be available in hard copy at each training session, and time will be provided to complete the evaluation at the conclusion of the course.

OMB is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

3. Enhance the quality, utility, and clarity of the information to be collected; and

4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

Analysis

Agency: Department of Homeland Security, National Protection and Programs Directorate.

Title: COML Prerequisite and Evaluation.

Form: Not Applicable.

OMB Number: 1670–NEW.

Frequency: On occasion.

Affected Public: State, local, or tribal government.

Number of Respondents: 3,000.

Estimated Time per Respondent: 15 minutes.

Total Burden Hours: 2,000 annual burden hours.

Total Burden Cost (capital/startup): $0.

Total Burden Cost (operating/maintaining): $48,840.00.

Dated: January 28, 2010.

Thomas Chase Garwood, III,

Chief Information Officer, National Protection and Programs Directorate, Department of Homeland Security.

[FR Doc. 2010–2298 Filed 2–2–10; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2009–0042]

Privacy Act of 1974; Department of Homeland Security/ALL—024 Facility and Perimeter Access Control and Visitor Management System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974 the Department of Homeland Security proposes to update and reissue Department of Homeland Security/ALL—024 Facility and Perimeter Access Control and Visitor Management System of Records to include record systems within the Federal Protective Service. Categories of individuals, categories of records, purpose and routine uses of this system have been reviewed and updated to better reflect the Department's, including the Federal Protective Service's, facility and perimeter access control and visitor management record system. The activities performed by the Department's facility and perimeter access control and visitor management systems often overlap with other security-related activities. Accordingly, data within each of the categories of individuals, categories of records, and routine uses may have similarities with other security-related systems of records, but each system is distinct based on its purpose.

Further, this system of records is separate from Department of Homeland Security/ALL 026—Personal Identity Verification Management System of Records, June 25, 2009, which supports the administration of the Homeland Security Presidential Directive—12 program, directing the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems while enhancing security, increasing efficiency, reducing identity fraud, and protecting personal privacy.

Records within this system apply only to perimeters and facilities where access is controlled by the Department of Homeland Security or its components, including the Federal Protective Service, and its contract guards.

Exclusion is made to perimeters and facilities secured by the U.S. Secret Service pursuant to 18 U.S.C. 3056 and 3056A and are not included under this system of records. Records pertaining to perimeters and facilities secured by the