information about unpublished patent applications.

This information collection includes the Certificate Action Form (PTO–2042), which is used by the public to request a new digital certificate, the revocation of a current certificate, or the recovery of a lost or corrupted certificate. Customers may also change the name listed on the certificate or associate the certificate with one or more previously assigned Customer Numbers. A certificate request must include a notarized signature in order to verify the identity of the applicant. The Certificate Action Form also has an accompanying subscriber agreement to ensure that customers understand their obligations regarding the use of the digital certificates and cryptographic software. When generating a new certificate, customers may provide additional information for a set of security questions and answers that will enable customers to recover a lost certificate online without having to contact USPTO support staff.

II. Method of Collection

The Certificate Action Form must be notarized and may be mailed or hand delivered to the USPTO. The Certificate Self-Recovery Form is submitted online through the USPTO Web site.

III. Data

OMB Number: 0651–0045.

Form Number(s): PTO–2042.

Type of Review: Extension of a currently approved collection.

Affected Public: Individuals or households; businesses or other for-profits; and not-for-profit institutions.

Estimated Number of Respondents: 4,126 responses per year.

Estimated Time per Response: The USPTO estimates that it will take the public approximately 30 minutes (0.5 hours) to read the instructions and subscriber agreement, gather the necessary information, prepare the Certificate Action Form, and submit the completed request. The USPTO estimates that it will take the public approximately 10 minutes (0.17 hours) to complete and electronically submit the information required for Certificate Self-Recovery.

Estimated Total Annual Respondent Burden Hours: 1,383 hours per year.

Estimated Total Annual Respondent Cost Burden: $167,343 per year. The USPTO expects that 70% of the submissions for this collection will be prepared by paraprofessionals, 15% by attorneys, and 15% by independent inventors. Using those proportions and the estimated rates of $100 per hour for paraprofessionals, $310 per hour for associate attorneys in private firms, and $30 per hour for independent inventors, the USPTO estimates that the average rate for those respondents will be approximately $121 per hour. Therefore, the estimated total respondent cost burden for this collection will be $167,343 per year.

Item	Estimated time for response (minutes)	Estimated annual responses	Estimated annual burden hours
Certificate Action Form (including Subscriber Agreement) (PTO–2042)	30	2,063	1,032
Certificate Self-Recovery Form	10	2,063	351
Totals	.....	4,126	1,383

Estimated Total Annual (Non-hour) Respondent Cost Burden: $4,992. There are no capital start-up costs, maintenance costs, or filing fees associated with this information collection. However, this collection does have annual (non-hour) cost burden in the form of recordkeeping costs and postage costs associated with the Certificate Action Form.

This collection has recordkeeping costs due to the notarization requirement for authenticating the signatures on the Certificate Action Form. The USPTO estimates that the average fee for having a signature notarized is $2 and that 2,063 responses for these forms will be submitted annually, for a total recordkeeping cost of $4,126 per year.

This collection also has postage costs for submitting the Certificate Action Form to the USPTO by mail. The form cannot be faxed or submitted electronically because it requires an original notarized signature for identity verification. The USPTO estimates that the first-class postage cost for these forms will be 42 cents and that it will receive 2,063 mailed responses annually, for a total postage cost of approximately $866 per year.

The total (non-hour) respondent cost burden for this collection in the form of recordkeeping costs and postage costs is estimated to be $4,992 per year.

IV. Request for Comments

Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and cost) of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, *e.g.*, the use of automated collection techniques or other forms of information technology.

Comments submitted in response to this notice will be summarized or included in the request for OMB approval of this information collection; they also will become a matter of public record.

Dated: October 16, 2008.

Susan K. Fawcett,

Records Officer, USPTO, Office of the Chief Information Officer, Customer Information Services Group, Public Information Services Division.

[FR Doc. E8–25280 Filed 10–22–08; 8:45 am]

BILLING CODE 3510–16–P

DEPARTMENT OF COMMERCE

Patent and Trademark Office

Privacy Act of 1974; System of Records

AGENCY: United States Patent and Trademark Office, Commerce.

ACTION: Notice of amendment of Privacy Act system of records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, as amended, the United States Patent and Trademark Office (USPTO) is amending the system of records currently listed under ''COMMERCE/PAT–TM–18 USPTO Identification and Security Access Control Systems.'' This action is being taken to revise the Privacy Act Notice to include the information necessary for identification

cards that meet the standards set by Homeland Security Presidential Directive 12 (HSPD–12) ''Policy for a Common Identification Standard for Federal Employees and Contractors'' (August 27, 2004). The system of records will also be renamed ''COMMERCE/PAT–TM–18 USPTO Personal Identification Verification (PIV) and Security Access Control Systems.'' We invite the public to comment on the amended system noted in this publication.

DATES: Written comments must be received no later than November 24, 2008. The proposed amendments will become effective on November 24, 2008, unless the USPTO receives comments that would result in a contrary determination.

ADDRESSES: You may submit written comments by any of the following methods:

- *E-mail: Calib.Garland@uspto.gov.*
- *Fax:* (571) 273–6247, marked to the attention of J.R. Garland.
- *Mail:* Calib P. Garland, Jr., Director of Security and Safety, United States Patent and Trademark Office, 551 John Carlyle Street 1A21, Alexandria, VA 22314.
- *Federal Rulemaking Portal: http://www.regulations.gov.*

All comments received will be available for public inspection at the Federal rulemaking portal located at *www.regulations.gov* and on the USPTO Web site at *www.uspto.gov.*

FOR FURTHER INFORMATION CONTACT: Calib P. Garland, Jr., Director, Office of Security and Safety, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313–1450, (571) 272–8000.

SUPPLEMENTARY INFORMATION: The United States Patent and Trademark Office (USPTO) proposes to revise an existing system of records that is subject to the Privacy Act of 1974. The system is entitled ''COMMERCE/PAT–TM–18 USPTO Identification and Security Access Control Systems,'' and was last published on December 14, 2004 (69 FR 74502). This system maintains information to produce photo identification cards for access to USPTO facilities as well as for building security, for identifying the bearer of the card as a Federal employee or contractor, for changing access permissions on cards, and for tracking stolen or lost cards. The system of records is being revised to describe the additional types of information being collected by the USPTO as required by Homeland Security Presidential Directive 12 (HSPD–12) ''Policy for a Common Identification Standard for Federal Employees and Contractors'' (August 27, 2004), which mandates a common identity standard for Federal employees and contractors on duty for more than six months.

The revised system of records is being renamed ''COMMERCE/PAT–TM–18 USPTO Personal Identification Verification (PIV) and Security Access Control Systems'' and is published in its entirety below.

COMMERCE/PAT–TM–18

SYSTEM NAME:

USPTO Personal Identification Verification (PIV) and Security Access Control Systems.

SECURITY CLASSIFICATION:

Sensitive but unclassified.

SYSTEM LOCATION:

Office of Corporate Services, Office of Security and Safety, United States Patent and Trademark Office, 600 Dulany Street, Alexandria, VA 22314.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

All agency employees, contractors, consultants, and volunteers who require routine, long-term access (180 days or more) to USPTO facilities, information technology systems, and networks. At its discretion, the USPTO may include short-term employees and contractors in the PIV ID program and, therefore, inclusion into the USPTO Personal Identification Verification and Security Access Control System (PIVSACS). The system does not apply to occasional visitors or short-term guests. The USPTO will issue temporary identification and credentials for those purposes.

CATEGORIES OF RECORDS IN THE SYSTEM:

Enrollment records maintained in the PIVSACS and on individuals applying for the PIV program and a PIV credential through the USPTO HSPD–12 system contained within the PIVSACS include the following data fields: Full name; Social Security number; employee ID number, date of birth; current address; digital color photograph; fingerprints; biometric template (two fingerprints); organization; employee affiliation; work e-mail address; work telephone number(s); copies of identity source documents; employee status; foreign national status; federal emergency response official status; results of background check; Government agency code; and PIV card issuance location. Records in the PIV ID Management System (IDMS) needed for credential management for enrolled individuals in the PIV program include: PIV card serial number; digital certificate(s) serial number; PIV card issuance and expiration dates; PIV card PIN; Cardholder Unique Identifier (CHUID); and card management keys.

Individuals enrolled in the USPTO PIVSACS will be issued a PIV card. The PIV card contains the following mandatory visual personally identifiable information: Name, photograph, employee affiliation, PIV card issue and expiration date, agency card serial number, and color-coding for employee affiliation. The card also contains an integrated circuit chip which is encoded with the following mandatory data elements which comprise the standard data model for PIV logical credentials: PIV card PIN, cardholder unique identifier (CHUID), PIV authentication digital certificate, and two fingerprint biometric templates. The PIV data model may be optionally extended to include the following logical credentials: Digital certificate for digital signature, digital certificate for key management, card authentication keys, and card management system keys. All PIV logical credentials can only be read by machine.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 35 U.S.C. 2; E.O. 9397; Federal Information Security Management Act (Pub. L. 107–296, Sec. 3544); E-Government Act (Pub. L. 107–347, Sec. 203); Government Paperwork Elimination Act (Pub. L. 105–277, 44 U.S.C. 3504); Homeland Security Presidential Directive 12 (HSPD–12) ''Policy for a Common Identification Standard for Federal Employees and Contractors'' (August 27, 2004).

PURPOSE(S):

The primary purposes of the system are to ensure the safety and security of USPTO facilities, systems, or information, and of facility occupants and users; to provide for interoperability and trust in allowing physical access to individuals entering other Federal facilities; and to allow logical access to USPTO information systems, networks, and resources.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside the USPTO as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To the Department of Justice when: (1) The agency or any component

thereof; (2) any employee of the agency in his or her official capacity; (3) any employee of the agency in his or her individual capacity where the agency 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, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.

b. To a court or adjudicative body in a proceeding when: (1) The agency or any component thereof; (2) any employee of the agency in his or her official capacity; (3) any employee of the agency in his or her individual capacity where the agency 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, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency 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, SF 85–P, and SF 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 about whom the record is maintained.

e. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

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), the Federal Information Security Management Act (Pub. L. 107–296), and associated Office of Management and Budget (OMB) policies, standards and guidance from the National Institute of Standards and Technology, and the General Services Administration.

g. To a Federal, state, local, or international agency, or tribal or other public authority, on request, in connection with the hiring or retention of an employee, the issuance or retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit, to the extent that the information is relevant and necessary to the requesting agency's decision.

h. To the OMB 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; and applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives.

j. To designated agency personnel for controlled access to specific records for the purposes of performing authorized audit or authorized oversight and administrative functions. All access is controlled systematically through authentication using PIV credentials based on access and authorization rules for specific audit and administrative functions.

k. To the Office of Personnel Management in accordance with the agency's responsibility for evaluation of Federal personnel management.

l. To the Federal Bureau of Investigation for the National Criminal History check.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Not applicable.

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

STORAGE:

Records are stored in electronic files.

RETRIEVABILITY:

Records may be retrieved by name of the individual, Cardholder Unique Identification Number, employee ID, and/or by any other unique individual identifier.

SAFEGUARDS:

Consistent with the requirements of the Federal Information Security Management Act (Pub. L. 107–296) and associated OMB policies, standards and guidance from the National Institute of Standards and Technology, and the General Services Administration, the USPTO Office of Security and Safety protects all records from unauthorized access through appropriate administrative, physical, and technical safeguards. Access is restricted on a ''need to know'' basis, utilization of PIV card access, secure network access, and card readers on doors and approved storage containers. The building has security guards and secured doors. All entrances are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; and pincode access screening. Personally identifiable information is safeguarded and protected in conformance with all Federal statutory and OMB guidance requirements. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. All data is encrypted in transit. The USPTO will maintain an audit trail and perform random periodic reviews to identify unauthorized access. Persons given roles in the PIV process must be approved by the USPTO and complete training specific to their roles to ensure they are knowledgeable about how to protect personally identifiable information.

RETENTION AND DISPOSAL:

Records retention and disposal is in accordance with the series records schedules. The records on government employees and contractor employees are retained for the duration of their employment at the USPTO. Other individuals' records are kept for the duration of their affiliation with the USPTO and then treated as employee

records. The records on separated employees are destroyed or sent to the Federal Records Center in accordance with General Records Schedule 18.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Office of Security and Safety, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313–1450.

NOTIFICATION PROCEDURE:

Information about the records contained in this system may be obtained by sending a request in writing, signed, to the system manager at the address above. When requesting notification of or access to records covered by this notice, requesters should provide the appropriate information in accordance with the inquiry provisions appearing in 37 CFR part 102, subpart B.

RECORD ACCESS PROCEDURES:

Requests from individuals should be addressed to the system manager at the address above. Individuals must furnish their full names for their records to be located and identified. See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

The general provisions for access, contesting contents, and appealing initial determinations by the individual concerned appear in 37 CFR part 102, subpart B. Requests from individuals should be addressed to the system manager at the address above. Individuals must furnish their full names for their records to be located and identified. See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

Employees, contractors, and other applicants, and those authorized by the subject individuals to furnish information.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: October 16, 2008.

Susan K. Fawcett,

Records Officer, USPTO, Office of the Chief Information Officer, Customer Information Services Group, Public Information Services Division.

[FR Doc. E8–25279 Filed 10–22–08; 8:45 am]

BILLING CODE 3510–16–P

DEPARTMENT OF DEFENSE

Office of the Secretary

Membership of the Defense Information Systems Agency Senior Executive Service Performance Review Board

AGENCY: Defense Information Systems Agency, DoD.

ACTION: Notice.

SUMMARY: This notice announces the appointment of members to the Defense Information Systems Agency (DISA) Performance Review Board. The Performance Review Board provides a fair and impartial review of Senior Executive Service (SES) Performance appraisals and makes recommendations to the Acting Director, Defense Information Systems Agency, regarding final performance ratings and performance awards for DISA SES members.

DATES: *Effective Date:* Upon publication of this notice in the **Federal Register**.

FOR FURTHER INFORMATION CONTACT: Ms. Patti Wai, SES Program Manager, Defense Information Systems Agency, P.O. Box 4502, Arlington, Virginia 22204–4502, (703) 607–4411.

SUPPLEMENTARY INFORMATION: In accordance with 5 U.S.C. 4214(c)(4), the following are the names and titles of DISA career executives appointed to serve as members of the DISA Performance Review Board. Appointees will serve one-year terms, effective upon publication of this notice.

Mr. John J. Penkoske, Jr., Director, Manpower, Personnel, and Security, DISA, Chairperson.

Ms. Paige R. Atkins, Director, Defense Spectrum Organization, DISA, Member.

Mr. Anthony S. Montemarano, Component Acquisition Executive, DISA, Member.

Mr. Jimaye H. Sones, Chief Financial Executive/Comptroller, DISA, Member.

Dated: October 15, 2008.

Patricia L. Toppings,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. E8–25301 Filed 10–22–08; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

Board of Regents of the Uniformed Services University of the Health Sciences

AGENCY: Department of Defense; Uniformed Services University of the Health Sciences.

ACTION: Quarterly Meeting Notice.

SUMMARY: Under the provisions of the Federal Advisory Committee Act of 1972 (5 U.S.C., Appendix, as amended) and the Sunshine in the Government Act of 1976 (5 U.S.C. 552b, as amended), this notice announces the following meeting of the Board of Regents of the Uniformed Services University of the Health Sciences (USU).

DATES: Tuesday, November 18, 2008, from 8:30 a.m. to 1 p.m.

ADDRESSES: Board of Regents Conference Room (D3001), Uniformed Services University of the Health Sciences, 4301 Jones Bridge Road, Bethesda, Maryland 20814.

FOR FURTHER INFORMATION CONTACT: Janet S. Taylor, Designated Federal Official, 4301 Jones Bridge Road, Bethesda, Maryland 20814; telephone 301–295–3066. Ms. Taylor can also provide base access procedures.

SUPPLEMENTARY INFORMATION:

Purpose of the Meeting: Meetings of the Board of Regents assure that USU operates in the best traditions of academia. An outside Board is necessary for institutional accreditation.

Agenda: The actions that will take place include the approval of minutes from the Board of Regents Meeting held August 5, 2008; acceptance of administrative reports; approval of faculty appointments and promotions; and the awarding of masters and doctoral degrees in nursing, the biomedical sciences and public health. The President, USU; Dean, USU School of Medicine; Dean, USU Graduate School of Nursing; Director, Armed Forces Radiobiology Research Institute; Director, Military Cancer Institute; and the President, USU Faculty Senate will also present reports. These actions are necessary for the University to pursue its mission, which is to provide outstanding health care practitioners and scientists to the uniformed services.

Meeting Accessibility: Pursuant to Federal statute and regulations (5 U.S.C. 552b, as amended, and 41 CFR 102–3.140 through 102–3.165) and the availability of space, this meeting is completely open to the public. Seating is on a first-come basis.

Written Statements: Interested persons may submit a written statement for consideration by the Board of Regents. Individuals submitting a written statement must submit their statement to the Designated Federal Official at the address listed above. If such statement is not received at least 10 calendar days prior to the meeting, it may not be provided to or considered