



Privacy Impact Assessment for the

**DHS Headquarters
DHScovery**

January 19, 2006

Contact Point

Jay A. Allen

Acting Advanced Distributive Learning Program Officer

Chief Human Capital Office

202-357-8421

Reviewing Official

Hugo Teufel III

Chief Privacy Officer

Department of Homeland Security

(571) 227-3813



Abstract

DHScovery is owned by the Office of the Chief Information Officer (OCIO) in partnership with the Office of the Chief Human Capital Officer (OCHCO). DHScovery will create an e-training environment that supports development of the Department of Homeland Security (DHS) workforce through simplified one-stop access to high quality e-training products and services. This privacy impact assessment (PIA) is being conducted because DHScovery collects personally identifiable information about DHS employees and contractors.

Introduction

The Office of Personnel Management (OPM) is responsible for the administration of the Enterprise Human Resources Integration (EHRI) e-Training Initiative. In order to implement the Initiative government-wide, OPM pre-approved certain training software vendors from which departments across the government may select a vendor who matches its needs. DHS selected OPM's GoLearn package as the solution for DHS's Department-wide e-training initiative.

Many of the current DHS components maintain and operate their own training systems. DHScovery's goal is to consolidate all training programs at DHS into a single operation.¹

DHScovery is intended to accomplish several objectives including:

- Providing easy access to mandatory and professional development training,
- Facilitating sharing of courses through a common DHS course catalog,
- Supporting the President's Management Agenda and the Office of Personnel Management's e-Training Initiative, and
- Meeting the reporting requirements of OPM and other federal oversight organizations.

DHScovery will manage the life cycle learning of DHS professionals. As illustrated in Figure 1 below, DHScovery acts as the gateway for learners, trainers, supervisors, and administrators to access the full range of DHS training, performance support, and other related services and systems available within the Department. DHScovery manages data such as student records, training histories, individual development plans, course catalogs, training resources, and required competencies.

DHScovery will interface with several third party content providers including SkillSoft, Books 24x7, and Ninth House. The content provider will host the course media on their servers and DHScovery will access the course content when prompted by a user. When the user completes or exits the course, the user's progress information including the successful or unsuccessful course completion information is sent from the content provider to the DHScovery.

¹ At this time this privacy impact assessment is not intended to address these legacy and component systems. Instead, this document focuses on the Headquarters training program and its intended target audience. The initial DHScovery audience will be Headquarters staff. Starting in fiscal year 2007, other components will migrate to DHScovery. This PIA will be modified as these legacy and component training products are consolidated.

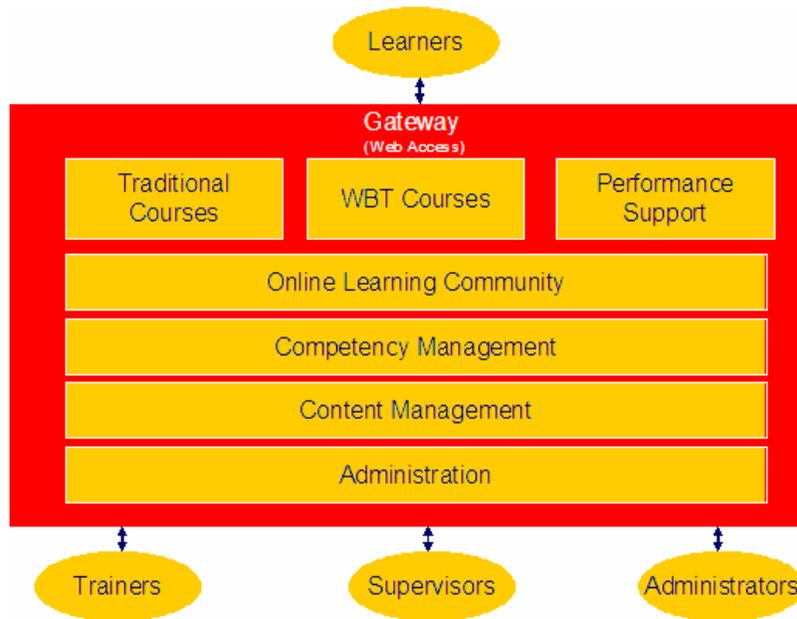


Figure 1. Role of the Headquarters DHScovery²

The ePerformance system is the only system that has supervisor direct report information for training requirements. The DHScovery system interfaces with the ePerformance system to retrieve supervisor and employee social security number.³ DHScovery utilizes the information from ePerformance to inform supervisors and employees of training requirements. DHScovery does not send information to ePerformance; it only receives information.

Additionally, the DHScovery system receives information from the National Finance Center (NFC). This information exchange includes employee demographic data e.g. employee’s organization identification, job position, and work location. See Section 1.1 for a detailed listing of NFC demographic data fields (marked by asterisk). This information is collected because the data fields that are supplied by NFC allow training administrators to appropriately assign and easily report on required training and career development metrics. DHS does not send any information to NFC; it only receives information.⁴

In a typical transaction, an employee will log onto DHScovery in order to complete training. The first time the employee logs into DHScovery he is prompted to change his username and password from the default and create a security question and answer.⁵ Once these items have been completed, the

² “WBT” is web-based training.

³PIA for ePerformance published June 21, 2005 and updated on October 13, 2006 at www.dhs.gov/privacy.

⁴ As a technical matter, prior to delivery to the DHScovery, the NFC import file is appended with the employee’s supervisor information that is contained in the E-performance System, by having a secure data transfers between DHS and the ePerformance production environment hosted at ServerVault. These data transfers will be used to support bi-weekly secure data transfer of NFC data to the production instance of the e-Performance system and annual performance rating data transferred from the e-Performance system. The diagram below illustrates the interface with e-Performance;

⁵ The default log-in convention is the first five (5) letters of the employee’s last name combined with the first letter of the employee’s first name. The password is the last four digits of the employee’s social security number in reverse. The employee must change the username to their DHS email address (dhs.gov domain is required) and change their password to conform with the parameters of the DHS password convention. If the employee does not change the default log-in information he cannot proceed with training.



employee is alerted to input his email address, which, in subsequent logins, becomes his login identification.⁶

Once the employee has successfully logged into the system they will be able to navigate to a catalog and launch a variety of self paced training selections. Once the employee successfully completes the training the system will record his training in the database and the user will be able to print a certificate of completion. Once the training has been recorded, supervisors, managers, and administrators will be able to run reports on training. Managers, supervisors, and administrators can also have the DHScovery application generate email notifications.

DHS is required to submit to OPM training-related data on a bi-weekly basis under the Enterprise Human Resources Integration Initiative. DHScovery will aid in more efficient reporting to OPM (see Question 1.1 and Section 5.0 for detail).

The vision of this initiative is to create a premier e-training environment that supports development of federal workforce through simplified and one-stop access to high quality e-training products and services, and thus advances the accomplishment of DHS's mission. This vision is supported by the following goals: (1) to support and advance the President's Management agenda by simplifying and unifying e-training services across government to improve the efficiency and effectiveness of government operations; (2) enhance agency human capital initiatives by supporting and /or leveraging existing e-training resources, and providing a focal point for their access across agencies that transforms the way government provides learning opportunities to employees; and (3) to advance continuous learning as a strategic business investment that promotes organizations agility, cost efficiencies; and improvements in performance.

Section 1.0: Information Collected and Maintained

1.1 What information is to be collected?

Employee Demographic Data collected by DHScovery (EHRI Data Fields):

- Last Name - The student's last name.*
- First Name - Students First name.*
- Middle Name - Student's Middle name.*
- Active/Inactive - If the User record is inactive, the employee will not be permitted to access the system and will be removed from some system searches and reports.
- Current Employment - Indicates the current employment status.^{7*}
- Employee Type - Indicates the employee relationship to DHS (e.g. Competitive-Career, SES Career, etc.).*

⁶ Personnel employee information is interfaced from the National Finance Center (NFC) database and the E-performance system into the DHScovery application database for the setup of user accounts as well as to manage and track training. NFC fields are required by DHS to automate the SF-182 process, be able to report training information to OPM or to report on statutory training completions to OCHCO. DHS supervisor personal information is pulled from the e-Performance system because the supervisor data is more accurate from this system than NFC. DHScovery only receives information from NFC and ePerformance and does not transmit information to NFC.

⁷ Active or inactive



- Job Series - The student's job series as identified by OPM.
- Job Title - The student's descriptive job title. This title provided insight into the day to day responsibilities of the employee.*
- Job Location*
- Job Description*
- Organization*
- Organization Description
- Hire Date*
- Term Date*
- Entry on Duty⁸
- Entry on Position⁹
- Entry on Management¹⁰
- Component Separation¹¹
- Date of Birth
- Pay Grade
- Pay Grade Step
- Education Level
- Supervisor
- Supervisor Status
- Training Histories ¹²
- Record Action – Indicates action¹³
- Social Security Number
- Birth date
- Enterprise Human Resources Integration (EHRI) ID – Unique number that EHRI will assign to an employee to identify employee records within the EHRI database.
- Agency Sub-element Code – Agency and where applicable the administrative sub-division in which a person is employed.

⁸ Appointments may not be effective prior to the date of approval by the appointing official. Additionally, appointments to positions in the civil service are effective only from date of acceptance and entrance on duty, unless a later date is stated on the Standard Form 52, Request for Personnel Action, or other approving document.

⁹ The start date in the student's current position. Format: mm/dd/yyyy

¹⁰ The start date for the student's current management position. Format: mm/dd/yyyy

¹¹ The last day of employment at the component for the student. Format: mm/dd/yyyy

¹² Course title, instructor, completion date, completion status, total

¹³ There are three types of record actions: Add, Correct, and Delete. The majority of records should be sent as Add type (Record Action = "A"). This will satisfy the normal reporting requirements for each training reporting period, and each record should include all fields in the training file specification).



- Training Title – Official title or name of the course or program completed by the employee.
- Training Type Code – Code for the type of training which has been completed.
- Training Sub Type Code – Code for the sub-type of training which has been completed by the employee.
- Training Start Date
- Training End Date
- Continued Service Agreement Expiration Date
- Continued Service Agreement Required Indicator – Indicates whether a continued service agreement is required for the training the employee is taking.¹⁴
- Training Accreditation Indicator – Indicates if the training course offers accreditation (if the course being offered is being offered by a accredited institution).
- Training Credit – Amount of academic credit hours or continued education units earned by the employee for the completed training.
- Training Credit Designation Type Code – Code for the type of academic credit hours or the continued education units earned by the employee for the completed training.
- Training Credit Type Code – Code for the type of credit hours received for the completed training.
- Training Duty Hours – Number of employee duty hours the employee used to complete the training unit.
- Training Non Duty Hours – Number of non-duty hours for the completed training course.
- Training Delivery Type Code
- Training Purpose type Code
- Training Source Type Code
- Training Materials Cost
- Training Per Diem Cost
- Training Travel Cost
- Training Tuition and Fees Cost

¹⁴ Each agency head determines the conditions for requiring employees to agree to continue in service after completing training e.g. 180 hours or more of Government or non-Government training. An employee selected for training must agree in writing with the Government before assignment to training to continue in service for a period at least equal to three times the length of the training period. 5 U.S.C. §4108(a)(1) (1997). If the employee leaves the Government before the agreed-upon amount of service, the agency has the right to require repayment for the amount of time not served. *Id.* at (b) and (c). The head of an agency may waive in whole or in part the agency's right of recovery if it is shown that the recovery would be against equity and good conscience or against the public interest. *Id.* at (c). For example, if an employee who is under a continued service agreement decides to voluntarily leave Federal service due to an impending reduction-in-force, the agency may determine that waiving its right to recovery would be in the public interest and release the employee from the agreement.

*This link is to the 1996 version of the document. To search for more recent updates select "Update" after following the link.



- Training Non-government Contribution Cost
- Username and Password

Information collected by content provider and provided to DHScovery:

- Attempt Number - The number of times the user has accessed the content lesson.
- Master Score - The overall score the user has received for the course.
- Maximum time allowed- The maximum time allowed to complete lesson.
- Time Limit Action- The time spent by user in the lesson.
- Lesson status - The completion status of the lesson.

Information collected by National Finance Center and provided to DHScovery (indicated by * above):

Employee demographic data in the DHScovery will be maintained by a system interface from DHS's Department wide HR database.¹⁵ DHS will be responsible for generating a Human Resources source file from NFC and delivering it to the DHScovery for import to the DHScovery database.

Information collected by the ePerformance system and provided to DHScovery:

- Supervisor Social Security Number

1.2 From whom is information collected?

Information is collected from any individual who is an employee of DHS and who has applied for, participated in, or assisted with a training program. The information is also collected from any other federal employee or private individual, including contractors and others, who has participated in or assisted with training programs recommended, sponsored, or operated by DHS.

DHScovery will be initially available only to DHS employees based on the number of available licenses for content. Contractors will be included in the system over time to meet mandatory training requirements.

1.3 Why is the information being collected?

In support of the President's Management Agenda and the DHS mission, information is being collected to ensure that DHS employees are being provided with the effective and current training opportunities required as part of a highly skilled Federal workforce. DHS's DHScovery has been designated to be the system of record for DHS wide training information.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

1. Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107-296, sec. 1512, 116 Stat. 2310 (Nov. 25, 2002),
2. Privacy Act of 1974 (5 U.S.C. 552a).

¹⁵ A standard SQL database.



3. EO 13111, Using Technology to Improve Training Technologies for Federal Government Employees.
4. E-Government Act of 2002 (Section 208).
5. Task Order Request for Quotation (TORFQ) # GL01-DHS-TORFQ-FY05-0001.

1.5 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated. For example, if during the design process, a decision was made to collect less data, include a discussion of this decision.

DHScovery collects only the information required to properly track and record training for DHS employees and contractors as well as to generate required OPM reports. Although the scope of information collected is large, each piece of data is required as part of the greater Human Capital training program in accordance with President's Management Agenda and the OPM's e-Training Initiative.

Because of the scope of information collected, DHScovery acknowledges that proper access controls are vital. Accordingly, access to the personally identifiable information collected or used by DHScovery is tightly guarded (see Section 8.0).

DHScovery uses social security numbers only in its interface with the NFC and ePerformance because it is the common and unique data element among the three systems. Within DHScovery the generated EHRI number is used. This ensures use of the social security numbers is minimal.

Section 2.0: Uses of the System and the Information

2.1 Describe all the uses of information.

The data collected by DHScovery will be used in the following ways:

- Courseware completion information will be collected to track and record that a given student has completed an assigned training event successfully.
- Supervisors may collect assessment information on their employees depending on mandatory training and other competency requirements.
- Schedule information will be collected for scheduled learning events.

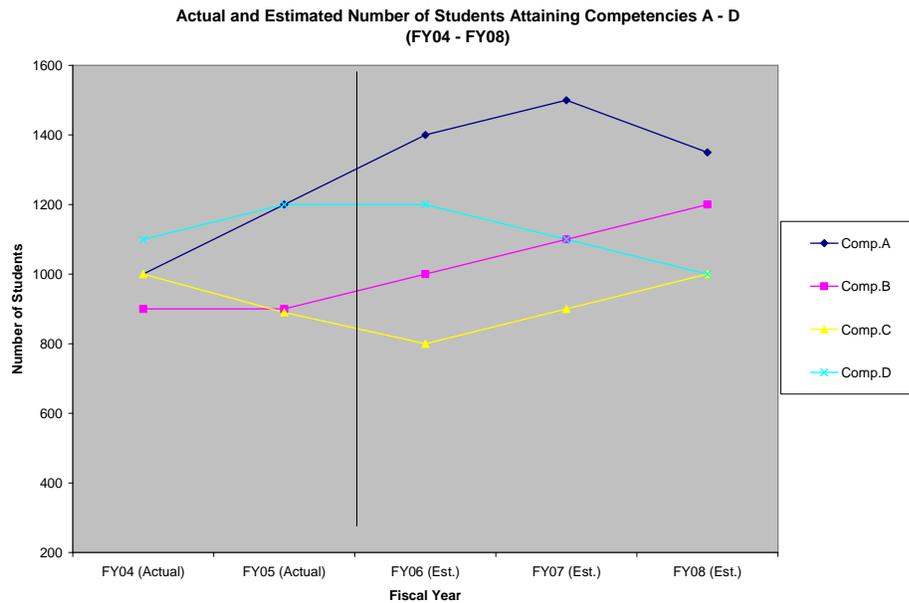
Students will be provided with detailed reports regarding their training progress, accomplishments, and future plans.

- All students will be provided with detailed information regarding the training content available to them.
- Supervisors and authorized training professionals will be provided with reports (as needed) regarding training accomplishments by their employees.
- DHScovery will contain some basic personal information (e.g., e-mail address, student identification number, etc.) for use in cross-referencing linked data sources.
- The mandatory EHRI data will be reported to OPM.



- Aggregate information will be collected and analyzed to identify patterns and trends to determine training effectiveness.

The below is an example of a typical aggregated data analysis report.



2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

Although the system does not inherently provide such functionality, the supporting DHScovery relational database could be accessed to perform aggregating analysis using reporting tools. See Appendix A for the types of reports that can be generated.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

The first time the user logs into DHScovery, he is prompted to update his password and create a security question and answer. Once these two items have been completed, the user is alerted to input his email address, which, in subsequent logins, becomes his login identification.

The user can update his contact information including work address, email address, and telephone number(s). The user can also update his regional information including the time zone and region location.

EHRI Training Data being reported to OPM will be matched against EHRI data in DHScovery. If the data does not match the EHRI training data it will be rejected by OPM.



2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses. For example, are audit logs regularly reviewed to ensure appropriate use of information? Are strict disciplinary programs in place if an individual is found to be inappropriately using the information?

Although there is a risk for misuse of information, all system users will have role-appropriate authentication information and will be trained regarding computer security and privacy. There will be a number of users in every DHScovery system role (including system administrator), enabling checks and balances for each role to ensure uses of the information are limited to those detailed in this privacy impact assessment and the System of Records Notice (SORN) for DHS General Training Records (71 FR 26767) (Appendix B). Finally, disciplinary action will be taken against any individual using information inappropriately, including criminal prosecution if warranted.

Section 3.0: Retention

3.1 What is the retention period for the data in the system?

As a preliminary matter DHS Headquarters Records Management Officer indicates a GRS Schedule 1-29 for training records will apply; however, all records are considered permanent until full evaluation by the DHS Headquarters Records Management Officer is accomplished. Full evaluation is expected in early 2007.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

NARA will evaluate records in system by 2007 after DHS completes its scheduling. All records are considered permanent until full evaluation is complete.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

DHScovery will have its records officially scheduled early in 2007. This will provide greater detail for the retention and disposal schedules. All records are considered permanent until officially evaluated. This policy ensures no federal records that might require NARA archiving are destroyed.



Section 4.0 Internal Sharing

4.1 With which internal organizations is the information shared?

The course catalog contained in DHScovery will be shared with each of the DHS components as DHScovery is distributed Department-wide. DHS components may share their course content with their subcomponents at their discretion. DHS components will only have access to personnel information that falls within their respective component. The DHScovery system only shares course content with components and subcomponents.

As discussed in the Introduction and Question 1.1, the ePerformance system will share supervisor social security numbers with DHScovery to notify supervisors of required training for their employees. The DHScovery will not share ePerformance data with any other system. DHScovery will receive data but never send data to ePerformance.

4.2 For each organization, what information is shared and for what purpose?

DHS components may share their course content with their subcomponents at their discretion but components will only employee name and course history if an employee moves from one component to another. This transfer will be handled by the designated and authorized personnel within each component. The DHScovery system only shares course content with components and subcomponents.

4.3 How is the information transmitted or disclosed?

Any information referenced in Question 4.1 would be transmitted or disclosed electronically via administrative changes performed within DHScovery and would follow appropriate security guidance for transfers of personally identifiable information.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated. For example, if a decision was made to limit internal sharing to certain components because of privacy or other concerns, include such a discussion.

The internal sharing discussed in this section would be performed strictly from within DHScovery. Information transfers would be a matter of enabling permissions for certain components and copying content from one catalog to another. These risks are mitigated by the role-based checks and balances discussed in Section 2.0 and Section 7.0. DHScovery does not send data to ePerformance; it only receives data. A very limited amount of personal information is used when an employee transfers components. This ensures that DHScovery's mission remains limited to training and efforts of DHScovery are not duplicative of other Human Capital efforts.



Section 5.0 External Sharing

5.1 With which external organizations is the information shared?

DHS is required to submit to OPM training-related data on a bi-weekly basis under the Enterprise Human Resources Integration initiative. Mandatory reporting requirements (EHRI Data, see Question 1.1) control which data will be shared with OPM.

DHScovery will also interface with content vendors (Skillsoft, Books 24X7, and Ninth House), but the content providers will not receive any personally identifiable information.

5.2 What information is shared and for what purpose?

DHScovery will receive employee demographic data updated on a nightly basis from the NFC payroll database. The data fields that are supplied by NFC, including the employee's organization, job position, and work location allow training administrators to appropriately assign and report on required training and career development metrics. DHScovery does not send data to the NFC.

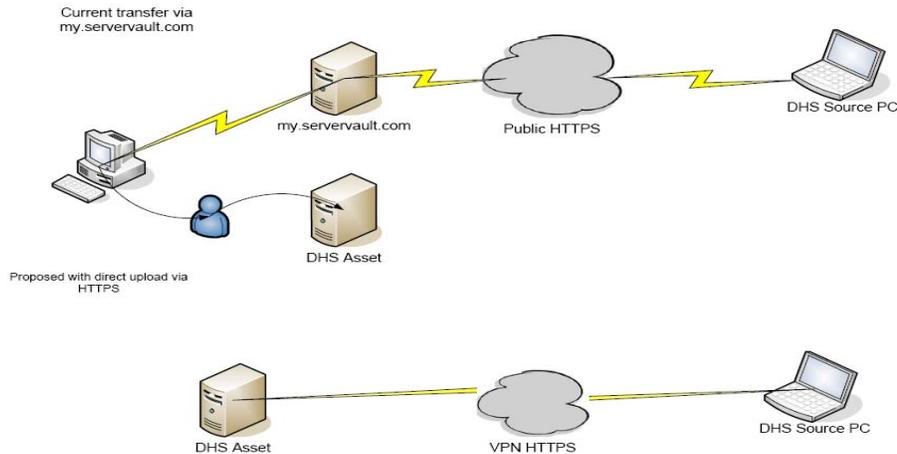
On a biweekly basis, the DHScovery will export training completion history to OPM's central training data repository as part of the EHRI integration. There are twenty-six required data elements for this initiative (see section 1.1 of this document, the first 26 data elements are the data elements reported to OPM and are noted by asterisk). Standard reports are discussed in Section 2.0 above.

DHScovery communicates with content vendors (SkillSoft, Books 24X7 and Ninth House) regarding the content of DHScovery courses. No personally identifiable information is exchanged.¹⁶

5.3 How is the information transmitted or disclosed?

All information is transmitted electronically. DHS will use encryption, Win-zip, and password protection on the source file. When a file is received the DHScovery will unzip the file using a password that has been previously provided and is stored in encrypted format in the DHScovery database in the tables. The source file will be uploaded to DHScovery at the hosting center by DHS using a firewall to firewall Virtual Private Network (VPN) secure connection.

¹⁶ Data exchanged with third-party content vendors: Attempt Number- The number of times the user has accessed the content lesson; Master Score- The overall score the user has received for the course; Maximun time allowed- The maximum time allowed to complete lesson; Time Limit Action- The time spent by user in the lesson; Lesson status- The completion status of the lesson



5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Because OPM is responsible for the administration of the e-Training Initiative under EHRI, OPM pre-approved three e-training solutions from which Departments could select their own e-training product. DHS Human Capital chose the GoLearn program from OPM's choices. The MOU with OPM GoLearn was co-signed by DHS CHCO and CIO in 2004. GoLearn provides the framework and technical support for DHScovery.

5.5 How is the shared information secured by the recipient?

The information is secured by SFTP (Secure FTP).

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

DHS provides security and privacy training to all DHS employees and contractors with access to DHScovery and ePerformance. As part of the U.S. Department of Agriculture, NFC users are required to have security and privacy training.



5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated. For example, if a decision was made to limit external sharing, include such a discussion.

The OPM human resources reporting requirements are government-wide, and as such, are afforded a high degree of rigor in establishing the appropriate mechanisms and protocols for data transmission. OPM requires the training information as part of its statutory duties. Information released to other external organizations will be done when an appropriate authority requests it and a secure means of transmission is established. The significant portion data is released in an aggregate form without personally identifying information (e.g., aggregate reports). Nonetheless, if personally identifiable information is exchanged the risks associated with improper disclosure or access are mitigated by the security controls in Section 8.0, as well as the secure connection (SFTP) used to transmit data.

Section 6.0: Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

A System of Records Notice specifically applicable to DHS's training efforts was published on May 8, 2006 in the Federal Register at 71 FR 26767 under the name "Department of Homeland Security General Training Records."

The notice given to employees prior to log-in reads as follows:

Privacy Act Notice: A System of Records Notice specifically applicable to DHS's training efforts was published on May 8, 2006 in the Federal Register at 71 FR 26767 under the name "Department of Homeland Security General Training Records." The authority to conduct training is derived from the Government Employees Training Act, 5 USC 4101-4118 as implemented by Executive Order 11348 of April 20, 1969, as amended by Executive Order 12107 (1978).

The system will automatically track and store any changes you make to your personal record and/or any other record you have the authority to change. These may include, but not limited to your login time and date, email address, your mailing address, and other editable information about you. The system will automatically track and store information about any online or external training you take through DHScovery. These include book marking, the scores you obtain in the training, cost of training etc.

Purposes and Use: The information you supply will be used to assist the government in retrieving information documenting your training. These records and information in the records may be used to: (1) disclose pertinent information to appropriate federal agencies when required to do so by law; (2) disclose information to a federal, state, or local agency, maintaining civil, criminal or other relevant enforcement



information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's or the bureau's hiring or retention decision concerning you, or the issuance to you of a security clearance, license, contract, grant, or other benefit; (3) disclosure of relevant information to a court, magistrate, or administrative tribunal in the course of presenting evidence.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

An individual may decline to provide information, however, if certain information is not provided, the employee may not receive credit for completing mandatory training. The employee is not requested to provide information beyond what is already in his personnel profile and that which was provided at hiring or security clearance.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

Consent to particular uses is defined in the notice given in the SORN for DHS General Training Records (71 FR 26767) and this PIA. Any uses outside that defined scope would require additional notice and consent; however, expansion of uses is not foreseen.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them. For example, if previously no notice was provided to the individual about how to correct information and you subsequently decided to provide this information, include a discussion of this decision.

Employees and contractors are on notice upon entering service to the Department that certain training may be required of them and, as part of that training, certain information may be required. It is important to note that the information provided is the same information already provided at hiring or security clearance. DHS OCHCO will not use personal information for purposes not contained within the SORN without first receiving approval from the Chief Privacy Officer to update the SORN and this PIA.

Section 7.0: Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

All DHScovery users must enter authentication information (username/password) to gain access to their information (Introduction and Question 1.1). Individuals may personally ensure that all of their biographic information is accurate. If an individual feels their biographic or training information is inaccurate a supervisor is required to verify and make appropriate changes.



7.2 What are the procedures for correcting erroneous information?

Users must notify their supervisors or the system administrator to correct erroneous information. The user can update their contact information, including work address, email address, and telephone number(s). The user can also update their regional information including their time zone and region location.

7.3 How are individuals notified of the procedures for correcting their information?

Users are provided this information initially during training, and then are provided these instructions onscreen through embedded help functions within DHScovery.

7.4 If no redress is provided, are alternatives are available?

Users may always contact their supervisors or the HQ DHScovery help desk for assistance in correcting whatever issues they may encounter.

Users may also contact the vendors' help desk for assistance.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, what procedural rights are provided and, if access, correction and redress rights are not provided please explain why not.

Procedural mechanisms for access and correction are included within the application itself and available as needed via an individual's supervisor. Notice is also given on the forms and websites associated with DHS training as well as in the Federal Register pursuant to the Privacy Act as well as this PIA. Also, individuals are aware that in their employment or involvement with DHS that training may be required in order maintain employment.

Section 8.0: Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

Classes of users include employees, supervisors, training specialists, training administrators, instructors, and system administrators.



8.2 Will contractors to DHS have access to the system?

Contractors will have access to the DHScovery over time, but not initially.

8.3 Does the system use “roles” to assign privileges to users of the system?

Yes.

8.4 What procedures are in place to determine which users may access the system and are they documented?

Users access to DHScovery falls in three general categories: (1) End users including DHS “learners” and their supervisors, (2) DHScovery administrative users (e.g. training coordinators, training managers, instructors, etc.), and (3) system administrators including database administrators, network engineers, etc.

End users (employees, supervisors) are granted login access to the application by an automated data feed from the NFC payroll database. If the DHS employee has an active record in the NFC and that record has been imported to DHScovery, then that employee will have access to DHScovery. Likewise, if the DHS employee has an active record in the DHScovery and leaves the government, their DHScovery account will be deactivated via an automated process during the next data upload from NFC. End user accounts can also be activated/deactivated by an administrative user of the system with the appropriate permissions (see next paragraph). End user access is documented in the DHScovery Design Document and also the NFC to Plateau Interface Technical Design Document.

Administrative users of the system must first request permission to have an account created from the DHScovery program manager. If approved an administrative account is created in the DHScovery application and a “Role” and data access permission level is assigned to the system user. Data access is controlled in DHScovery by domains and workflows (a “role” is a collection of workflows) A domain sets what data can be accessed by an administrator and a workflow establishes what the administrator can do with that record in the database (e.g. add curriculum, edit online content, etc.). Domain access and administrative roles are configured in the system according to the business requirements set forth by the DHS Program Manager. These business decisions are documented in the DHScovery Solution Design Document.

System administrators are employees of Plateau Systems, Ltd. and Verizon IP Business Solutions that are responsible for the actual software and hardware the DHScovery system operates on. Personnel having system level access to the DHScovery must first submit to a background investigation and go through the government security clearance process according to the DHS Management Directive 11055 Suitability Screening Requirements for Contractors.

These procedures are documented in the System Security Plan.



8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

DHScovery administrative roles are reviewed through a series of workshops with the appropriate DHS training program managers and are documented in the Configuration Solution Design Document. Next, the roles and their associated data access permissions are tested during User Acceptance Testing prior to bringing the system into production. The DHScovery System Security Plan documents these procedures.

At the system level, access to back-end servers is restricted to unique logins in order to maintain a trail of system administrator access.

Employee and supervisor roles are verified and updated through the ePerformance system. Within ePerformance employees select their supervisor. Should an employee take on supervisor status or should an employee's supervisor change, ePerformance updates would update DHScovery automatically.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

- Data access is controlled in DHScovery by domains and workflows (a "role" is a collection of workflow.) A domain sets what data can be accessed by an administrator and a workflow establishes what the administrator can do with that record in the database (e.g. add curriculum, edit online content, etc.).
- To access the DHScovery as either an administrator or as an end user, the individual must have a valid and active account. Encrypted passwords are stored in DHScovery database and conform to the DHS password complexity rules. Passwords must also be updated every ninety (90) days. System access is denied after three unsuccessful login attempts in one hour.
- DHScovery also has over one hundred (100) audit tables that provide full audit capability for data changes to all major data entities.
- Intrusion detection systems are deployed at the enclave boundary and at layered or internal enclave boundaries. Similarly, full audit capability is enabled, including normal system administrator access as well as any unauthorized-user activity.
- In addition there is a continuous on-line monitoring and audit trail creation capability for all firewalls deployed with the capability to immediately alert personnel of any unusual or inappropriate activity.
- The system maintains audit trails for all data that would be required to establish the complete set of assignment and history data for an individual.



8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

DHS provides the necessary training to all appropriate personnel including privacy and computer security training.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The Office of Personnel Management, the Application Service Provider, has issued an Authority to Operate (ATO) letter dated August 7, 2006 for Plateau (software vendor)/Verizon (hosting site) DHScovery (under the name Learning Management System).

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated. For example, if a decision was made to tighten access controls by restricting access to specific users, include such a discussion.

As described above robust auditing and access measures have been implemented. Taken together these two measures mitigate the risk of unauthorized access and use. DHScovery has met the Department's system security standards.

Section 9.0: Technology

9.1 Was the system built from the ground up or purchased and installed?

OPM GoLearn was selected as the best solution to DHS's e-training needs. System configuration will need to be completed to align with Headquarters organizational structures and workflows. The current launch date for the DHScovery is February 5, 2007.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

DHS has confirmed that the analysis was performed by OPM GoLearn prior to its pre-selection. Both commercial off-the-shelf DHScovery products currently under consideration were successful GoLearn vendors, and have passed such examination. The information system is based on potential impact of system/data confidentiality, integrity, availability, and the information processed stored, or transmitted by the system in accordance with Federal Information Processing Standards Publication 199 and National Institute of Science and Technology Publication 800-60.



9.3 What design choices were made to enhance privacy?

DHS has not been directly involved in making any such design choices, and relies instead on the experience and discretion of OPM GoLearn in ensuring appropriate technical solutions; however, DHS was given three choices in regard to technology selection, and GoLearn was deemed to be the option that not only accomplished mission needs, but also was most capable of securing employee data in a manner sensitive to privacy concerns. To the extent DHS was given the choice by OPM, DHS has chosen the option that best accomplishes its goals and best protects employee and contractor privacy.

Responsible Officials

Jay A. Allen
Advanced Distributive Learning Program Officer
Chief Human Capital Office
202-357-8421

Approval Signature

_____ January 19, 2006

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security



Appendix A. DHScovery Standard Reports

The Plateau standard reporting feature contains 68 reports. Each report menu gives options of grouping and sorting outputs in various ways. A sampling of reports is highlighted below. In addition to these standard reports, the system allows users to create custom reports, external reports, recurring report jobs, saved reports and background report jobs. All reports are downloadable into XML, CSV, HTML and PDF formats.

User Management Reports

- **Account Data:** The Account Data report shows a repository of information concerning the item:
 - Summary version includes only basic Human Resources-type information for the Users specified.
 - Detail version includes a comprehensive report of the Users' curriculum status, current item needs and required dates, competency profile assignments, assigned competencies with required and assessed mastery levels, and the User's training history.
- **Certificate of Completion:** The Certificate of Completion is a program that can be used to print certificates of completion for selected items and Users. The certificates can be printed on blank and white paper or custom paper stock.
- **Certificate of Completion for Offerings:** The Certificate of Completion is a program that can be used to print certificates of completion for selected items and Users. The certificates can be printed on blank and white paper or custom paper stock.
- **Competency Assessment:** The User Competency Assessment Report displays, for the users and competencies selected for the report, the user's required mastery level, his assessed mastery level, and for each competency, the date of the last assessment. It is possible to group the report output either by user or by competency, and can mask user IDs if necessary. Grouping the report by user is a convenient way to view the competency profile of each user included in the report.
- **Competency Profiles Status:** The User Competency Set Status Report displays, for the users and competencies selected for the report, the date when the competency profile was assigned to the user and whether or not the user has completed the requirements of the competency profile. It is possible to group the report output either by user or by competency profile, can show competency detail, and mask the user IDs, if necessary.
- **Conflict:** The User Conflict report shows the dates, times and schedule offerings conflict for the specified Users.
- **Cumulative Gap Analysis:** The Cumulative Gap Analysis Report displays, for the users and competencies selected for the report, the average gap between the user's assessed ability and the mastery level required in the user's competency profile. This is a statistical summary report for the selected users; no individual user information will be shown unless the person running the report chooses to run the report for only one user at a time.
- **Curriculum Item Status:** The User Curriculum Status Item Report shows you, or the users and curricula selected for the report, the curriculum assigned to each user and their items. The



completion date, completion status, and required date for each item are included. You can also choose to mask the user IDs if necessary.

- **Curriculum Status:** The User Curriculum Status report displays the curriculum status of the selected User(s) for the selected curriculum(s). The report will display curriculum that are complete, incomplete or both. The report will also display the status at an item detail level.
- **External Request Data:** The External Request Data report shows all information related to external requests that are made.
- **External Request Tuition:** The External Request Tuition report shows all external requests for tuition fees.
- **Item Status:** The User Item Status report shows each User's completion status for the items they participated in during the date range specified. If no date range is specified, all records will be included. Substitute relationships and other completion statuses can also be displayed in this report.
- **Job Position Detail:** The Job Position Detail Report shows you, for each job position included in the report output, the curricula and/or competency profiles to which it is related.
- **Learning History:** The User Learning History report shows the learning events in which the User participated during the date range specified. The output is always grouped by item.
- **Learning Hours:** The User Learning Hours report shows the total number of "hours" of a specified type that the User has completed. The report can show total hours by credit hours, CPE hours, contact hours or total hours.
- **Learning Needs:** The User Learning Needs report shows the Users' outstanding training requirement(s) for the item or items specified. Required dates of training for each item are also included, where applicable.
- **Learning Plan:** The User Learning Plan report shows the items that are included in a User's development plan, required dates, and whether/when the User has completed the item. The report is organized by User and can be sorted chronologically, by item or by curriculum.
- **Online Item Status:** The User Online Item Status report shows the User's current progress through online items. The report is organized by item, so the status of all Users in that item can be viewed before any individual User's status is reported. A User's progress through an online course is reported at the content module level of detail.
- **Organizational Assessment Data:** This report lists information about organizations and their related competencies.
- **Region Data:** The Region Data report shows the facilities located within the region, and the instructors that have been assigned to the region.



- **Self-Registration/Withdrawal:** The User Self-Registration/ Withdrawal report shows each User's ID, name, the schedule ID, the related items, registration status, registration cut off date, tuition refund date, and registration date. User can be selected based on multiple criteria.
- **User Created Account:** The User Self-Registration report shows the User ID, name, date and time the self-registration record was created, and the User's phone number.
- **User Costs:** The User Costs report returns information about each selected user's cost for each item that they have completed.

Learning Reports

- **Class Data:** The Class Data report displays all of the information about a class. This includes the basic information such as description, domain, and maximum capacity. It also includes the custom columns, the related Users, and the related scheduled offerings.
- **Class Location:** The Class Location report displays, by class and by date, where a User in the class is supposed to be on a given date. The report shows the Users and the schedule offering segments on the axis of a matrix, and the location that the User was supposed to be for the segment
- **Class Progress:** The Class Progress report displays, by class, the progress of all of the Users in a class. The report shows the Users and the schedule offerings of the class in a matrix format, with the completion status of each offering for each User inside the matrix.
- **Class Roster:** The Class Roster report shows the instructor and Users who have been scheduled. The report provides space for Users who are on the registration list to sign their names and date their signatures.
- **Curricula with Related Job Positions:** The Curriculum with Related Job Position report shows which job positions include the curriculum. The report is always grouped by curriculum.
- **Curriculum Data:** The Curriculum Data report shows the curriculum's domain, whether or not it is active, the date of creation, and some detail about any related items, job positions, and documents.
- **Custom Resource Data:** The Custom Resource Data report shows any base or additional costs associated with the custom resource selected.
- **Document Data:** The Document Data report displays all of the data stored the document records that are included in the report, including the document type, source, location, revision and approval information. All linkages between a document, and tasks, curricula, and items, are listed on the report.
- **Document Review Flag:** The Document Review Flag report shows whether the relationship between the documents that are listed in the report and any tasks, curricula, and items for the documents you include in the report, should be reviewed because of a revision.
- **Equipment Data:** The Equipment Data Report provides you with a separate page of information for each individual piece of equipment of the equipment types that you include in the report. The report shows for each equipment, the ID, Serial Number, Assigned Location, Status, Domain, and Hourly Cost of operation.
- **Equipment Status:** The Equipment Status report provides you with a separate line of information for each individual piece of equipment of the equipment types and statuses that



you include in the report (you must provide both criteria in order to run the report). The report includes each item's ID, assigned location, status, and domain.

- **Equipment Utilization:** The Equipment Utilization Report shows you, for the equipment types you select within a specified date range, the number of offerings for which each individual piece of equipment has been scheduled, and the total number of hours the equipment is scheduled to be in use.
- **Instructor Data:** The Instructor Data report shows the instructor's cost per hour, e-mail address, items the instructor is qualified to teach, and other system management information.
- **Instructor Proctor Codes:** The Instructor Proctor Codes report prints the proctor codes for the date range and instructors specified. The report can be sent to proctors for reference.
- **Item Data:** The Item Data report displays item data. If many items will be included in a detail report, the result can be quite lengthy.
- **Item List:** The Item List report shows the item type and item ID, the revision date, and the title.
- **Item Object Details:** The Item Object Details report contains details about the groups of content objects, the content objects themselves, and exams or surveys that are included in the online item.
- **Item Requests:** The Item Requests report shows which Users have requested which items but have not yet been enrolled or waitlisted in a schedule offering of the item.
- **Item Type List:** The Item Type List Report shows you, for the item(s) you have selected to include in the report, the item type and item ID, the revision date, and the title.
- **Items with Prerequisite Items:** The Items with Prerequisite Items report lists those items that have been defined as prerequisites.
- **Items with Related Documents:** The Items with Related Documents report shows the documents related to the item(s). The output is always grouped by item; you cannot change the default grouping.
- **Learning Calendar:** The Learning Calendar report shows all the training events scheduled for the day. The report output is shown in a table, rather than in calendar format.
- **Material Data:** The Material Data Report shows you, for each material type included in the report, the facilities where inventories of the material type are traced, and the items in which the material type is used. The facility data includes the current inventory level and the reorder point.
- **Registration Status:** The Registration Status report shows a detailed list of registration information. When grouped by instance, it might make a great class roster for an instructor. When grouped by User, it takes on the appearance of a class schedule for each individual User.
- **Resource Conflict:** The Resource Conflict report shows existing scheduling conflicts involving locations, instructors, and equipment. The basic organization of this report cannot be changed. It is divided into three groups: one for each of the resource types upon which it reports.
- **Schedule Offering Data:** The Schedule Offering Data report shows detailed information about each existing schedule offering including the item scheduled, dates scheduled, registration and waitlist data, instructor data, segment data, and delivery costs.



- **Slot Status:** The Slot Status report shows the current status of any slots that have been purchased. Where User names have been identified to fill the slots, the User names are included on the report, along with the registration status and schedule information.
- **Substitute Relationship:** The Substitute Relationship report shows those items for which a substitute relationship has been established, and what completion status goes on a User's record when he or she is given credit for completing an item via substitute.

Content Reports

- **Exam/Survey Objects:** The Exam/Survey Objects Report shows you, for all the exams and surveys you choose to include on the report, a summary of the exam or survey's features and design, such as the objectives and questions covered by the exam or survey, the passing grade required for the overall exam and for each objective, the number of minimum and maximum questions from each objective, and the scoring weight (see Points column on output) assigned to each objective and to each question that has been included independently from any objective. The report also shows what actions will be taken that depends upon a user's passing or failure upon completion.
- **User Exam/Survey Data:** The User Exam and Survey Data Report shows you, for all the users, exams and surveys you choose to include on the report, the details of users' performance on exams and surveys, including external exams. You can choose whether the report should include details of the user's performance with regard to individual questions, to the exam's associated objectives, and even to print each question on the report.
- **Exam/Item Analysis:** The Exam Item Analysis Report describes exams in the system by their questions. Each instance of an exam appears with the questions that were associated with the exam at run time. Remember that the exams can be randomized, and the questions are drawn from a pool. So even though a user only sees 5 questions, there could be 10 questions in the pool. In the report, all the questions in the pool appear but not every question appeared in every instance of an exam taken by a user.

System Admin Reports

- **Approval Process Data:** The Approval Process Data report shows related approval process data such as; the Process ID, Process Name, Version, Domain ID, Owner Email, Process steps, etc. The report also shows the Items and Scheduled Offerings related to the Approval Process.
- **Approval Role Coverage:** The Approval Role Coverage report shows the users and the approval role assigned to approve their items and scheduled offerings.
- **Approval Role Data:** The Approval Role Data report shows the approval processes assigned to each role, the users that are tied to the process, as well as related approval data information such as; approval role ID and description.
- **Approvals Status:** The Approvals Status report shows all information related to approvals. Information includes items and scheduled offerings submitted for approvals and their related status (approved, denied, etc.)
- **Facility Data:** The Facility Data report shows the management and identifying information of each facility record included on the report. It then lists each facility's location, assigned equipment, and material types, quantity on-hand, and reorder level.



- **Holiday Profile:** The Holiday Profile Report shows you, for each holiday profile selected, the facilities to which it has been applied; and the names, dates, and database ID of each holiday that is included in each profile. It is important to note that new holiday profiles must be created for each calendar year.
- **Location Data:** The Location Data report shows management data for each location you include in the report; include location type, domain, capacity, operating cost rate, and any equipment that is assigned to the location.
- **Location Utilization:** The Location Utilization report shows the number of schedule offerings in each location listed on the report and the total number of hours associated with those schedule offerings. The report is organized by location type.



Appendix B

[Federal Register: May 8, 2006 (Volume 71, Number 88)]
[Notices]
[Page 26767-26769]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr08my06-55]

=====
=====

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2006-0017]

Privacy Act of 1974: System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security is giving notice that it proposes to add a new system of records to its inventory of record systems for Department of Homeland Security General Training Records.

DATES: Comments must be received on or before June 7, 2006.

ADDRESSES: You may submit comments, identified by docket number DHS-2006-0017, by one of the following methods:

Federal eRulemaking Portal: http://www.regulations.gov. Follow the

instructions for submitting comments.

Fax: (571) 227-4171 (This is not a toll-free number).

Mail: Maureen Cooney, Acting Chief Privacy Officer, DHS Privacy Office, Mail Stop C-3, 601 S. 12th Street, Arlington, VA 22202-4220.



Instructions: All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change and may be read at <http://www.regulations.gov>, including

any personal information provided.

FOR FURTHER INFORMATION CONTACT: Maureen Cooney, Acting Chief Privacy Officer, Department of Homeland Security, by telephone (571) 227-3813 or facsimile (571) 227-4171.

SUPPLEMENTARY INFORMATION: Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107-296, section 1512, 116 Stat. 2310 (Nov. 25, 2002), the Department of Homeland Security (DHS) and its components and offices have relied on preexisting Privacy Act systems of records notices for the maintenance of records that concern training of current and former Departmental employees, contractors, and other individuals. See, e.g., CS.238, Customs Service Training and Career Individual Development Plans and C.239, Customs Service Training Records, last published on October 18, 2001 at 66 FR 2984.

As part of its efforts to streamline and consolidate its record systems, DHS is establishing a new agency-wide system of records under the Privacy Act (5 U.S.C. 552a) for the Department of Homeland Security (DHS) General Training Records. This record system will allow all component parts of DHS to collect and preserve training records under one centralized system. The system will consist of both electronic and paper records and will be used by DHS and its components and offices to maintain records about individual training, including enrollment and participation information, information pertaining to class schedules, programs, and instructors, training trends and needs, testing and examination materials, and assessments of training efficacy. The data will be collected by employee name or other unique personal identifier. The collection and maintenance of this information will assist DHS in meeting its obligation to train its personnel, contractors, and others in order to ensure that the agency mission can be successfully accomplished.

The Privacy Act embodies Fair Information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates personally identifiable information. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Individuals may request their own records that are maintained in a system of records in the possession or under the control of DHS by



complying with DHS Privacy Act regulations, 6 CFR 5.21.

The Privacy Act requires that each agency publish in the Federal Register a description denoting the type and character of each system of records in order to make agency recordkeeping practices transparent, to notify individuals about the use to which personally identifiable information is put, and to assist the individual to more easily find files within the agency.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this revised system of records to the Office of Management and Budget and to the Congress.

System of Records

DHS/All-003

System Name:

Department of Homeland Security General Training Records.

Security Classification:

Unclassified; sensitive.

System Location:

Records are maintained at several Headquarters locations and in component offices of the Department of Homeland Security, in both Washington, DC and field locations.

This system of records will cover:

1. Any individual who is or has been an employee of DHS and who has applied for, participated in or assisted with a training program;
2. Any other Federal employee or private individual, including contractors and others, who has participated in or assisted with training programs recommended, sponsored or operated by the Department of Homeland Security.

Authority for Maintenance of the System:

The Homeland Security Act of 2002, Public Law 107-296, 6 U.S.C. 121; Federal Records Act, 44 U.S.C. 3101; 6 CFR Part 5; 5 U.S.C. app. 3; 5 U.S.C. 301 and Ch. 41; Executive Order 11348, as amended by Executive Order 12107; and Executive Order 9397 (SSN).

Categories of Individuals Covered by the System:

Current and former employees of DHS, volunteers and contractors; other participants in training programs, including instructors, course developers, observers, and interpreters.

Categories of Records in the System:

The system includes all records pertaining to training, including



nomination forms; registration forms; course rosters and sign-in sheets; instructor lists; schedules; payment records, including financial, travel and related expenditures; examination and testing materials; grades and student evaluations; course and instructor critiques; equipment issued to trainees and other training participants; and other reports pertaining to training. Names and social security numbers are included in these records. Records of individuals who apply for but are not

[[Page 26768]]

accepted for training may also be included in this system.

Purpose:

This record system will collect and document training given to DHS employees, contractors and others. It will provide DHS with a means to track the particular training that is provided, identify training trends and needs, monitor and track the expenditure of training and related travel funds, schedule training classes and programs, schedule instructors, track training items issued to students, assess the effectiveness of training, identify patterns, respond to requests for information related to the training of DHS personnel and other individuals, and facilitate the compilation of statistical information about training.

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 DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. When a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil or administrative, the relevant records may be referred to an appropriate Federal, State, territorial, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting such a violation or enforcing or implementing such law.

B. To a Federal, State, tribal, local or foreign government agency or professional licensing authority in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance or status of a license, grant, or other benefit by the requesting entity, to the extent that the information is relevant and necessary to the requesting entity's decision on the matter.



C. To the news media and the public where there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of the Department or is necessary to demonstrate the accountability of the Department's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

D. To the National Archives and Records Administration or other federal government agencies in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

E. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

F. To the Department of Justice or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) DHS, or (b) any employee of DHS in his/her official capacity, or (c) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee, or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that disclosure is relevant and necessary to the litigation.

G. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

H. To educational institutions or training facilities for purposes of enrollment and verification of employee attendance and performance.

I. To an agency, organization, or individual for the purposes of performing authorized audit or oversight operations.

J. To the Equal Employment Opportunity Commission, Merit Systems Protection Board, Office of the Special Counsel, Federal Labor Relations Authority, or Office of Personnel Management or to arbitrators and other parties responsible for processing any personnel actions or conducting administrative hearings or appeals, or if needed in the performance of authorized duties.

K. To the Department of Justice or a consumer reporting agency for further action on a delinquent debt when circumstances warrant.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records in this system are stored electronically or on paper in secure facilities. The records are stored on magnetic disc, tape, digital media, and CD-ROM, and may also be retained in hard copy format



in secure folders.

Retrievability:

Data may be retrieved by the individual's name, Social Security Number, other personal identifier.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. The system maintains a real-time auditing function of individuals who access the system.

Retention and Disposal:

Records are maintained and disposed in accordance with National Archives and Records Administration General Records Schedule, No. 1.

System Manager(s) and Address:

The records are maintained at the Headquarters offices of the Department of Homeland Security in Washington, DC and in component offices located in Washington and elsewhere.

Notification Procedure:

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing to the DHS Privacy Officer at the U.S. Department of Homeland Security, Privacy Office, Arlington, Virginia 22202 or to the respective DHS component or office where the records are maintained.

Record Access Procedure:

See "Notification Procedure" above.

Contesting Record Procedures:

See "Notification Procedure" above.

Information contained in the records is obtained from employees, contractors, volunteers and others and from government and non-government organizations and individuals that provide training to agency employees.

Exemptions Claimed for the System:

Certain records in this system may be exempt on the basis of 5 U.S.C. 552a(k)(6) in order to preserve the



[[Page 26769]]

objectivity and fairness of testing and examination material.

Dated: April 28, 2006.
Maureen Cooney,
Acting Chief Privacy Officer.
[FR Doc. E6-6809 Filed 5-5-06; 8:45 am]

BILLING CODE 4410-10-P