Privacy Impact Assessment
for the

Department of Justice

Plateau Learning Management System (LMS)

Combined for the Instances listed:

ATF-learnATF

DEA-DEALS

DOJ-learnDOJ

May 26, 2010

Contact Point (ATF)
Wendy L. Frederick
Learning Systems Management Division
Office of Training and Professional Development
Bureau of Alcohol, Tobacco, Firearms and Explosives
202-648-8397

Contact Point (DEA)
Michele R. Norris
Learning Technologies Program Manager
Office of Training
Drug Enforcement Administration
703-632-5159

Contact Point (JMD)
Al Stiles
Enterprise Learning Technologies Program Officer
Justice Management Division/Human Resources Staff
Department of Justice
(202) 353-1605

Reviewing Official
Vance Hitch
Chief Information Officer
Department of Justice
(202) 514-0507

Approving Official
Nancy Libin
Chief Privacy and Civil Liberties Officer
Department of Justice
(202) 307-0697

Introduction

The Department of Justice Learning Management System (LMS) Architecture supports agency efforts in relation to Office of Personnel Management (OPM) Guide to Human Resources Reporting (Enterprise Human Resource Reporting Integration – EHRI) and the e-Government Human Resources Line of Business – Human Resource Development (HR LoB/HRD). This combined assessment is for the three branded sites of the Department of Justice's (DOJ) Learning Management System (LMS) which are based on a single Plateau LMS instance contracted through the Office of Personnel Management (OPM) and the National Technical Information Service (NTIS) and located at an OPM contracted server facility. The three branded sites of the LMS covered by this assessment are the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) LMS called learnATF, the Drug Enforcement Administration (DEA) LMS called DEALS and the Justice Management Division (JMD) LMS called learnDOJ. The LMS is based on a Commercial Off-The-Shelf (COTS) software application that manages web-based and classroom-based learning activities. The major functions of the LMS include providing access to commercial and Component-specific web-based courseware, managing an on-line catalog of course offerings; automating training registration and approval processes; on-line individual development planning; on-line testing and surveys; tracking of training resources; management of and reporting on training data; and tracking of training certifications. The LMS is hosted externally at an OPM/GoLearn approved hosting facility. GoLearn and NTIS are OPM approved HR LoB/HRD Customer Service Providers (CSPs). Office of Management and Budget (OMB) and OPM require all Federal agencies to use an OPM approved CSP to provide LMS services and meet HR LoB/HRD requirements. OPM GoLearn issues and maintains the Certification and Accreditation (C&A) for this LMS. This assessment describes the DOJ's use of an LMS contracted through OPM and NTIS. The overall LMS Architecture is shown in **Appendix A**.

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

LearnATF is used to collect information on the training and development conducted or sponsored by ATF for its employees, contractors, task force officers and State, local and international law enforcement partners. Key records that contain information about individuals include those for learners, instructors, and LMS administrators. For federal employee learners and instructors, this data includes names, work address, other information publically available on federal employees, as well as gender and Race and National Origin (RNO) on learners pursuant to EEOC Management Directive 715. RNO data is maintained in a privacy table not accessible to anyone through the application interface except for defined personnel/EEO staff. See Appendix B for data tables listing all information collected for learner, instructor and administrator records for learnATF.

LearnDOJ is used to collect information on the training and development conducted or sponsored by JMD for their employees and contractors. Key records that contain information about individuals include those for learners, instructors and LMS administrators. For learners, this information includes names, work address, other information publically available on federal employees, and the last four digits of Social Security Number (SSN). Information about RNO and gender are not collected. See **Appendix C** for data tables listing all information collected for learner, instructor and administrator records for LearnDOJ.

DEALS is used to collect information on the training and development conducted or sponsored by DEA for their employees, contractors, and task force officers who supervise DEA employees. Key records that contain information about individuals include those for learners and LMS administrators. DEA will collect information about instructors in the future. For learners, this information includes names, work address, other information publically available on federal employees, and the last four digits of Social Security Number (SSN). Information about RNO and gender are not collected. See **Appendix D** for data tables listing all information collected for learner, instructor and administrator records for DEALS. DEA plans to track state and local law enforcement officials that take particular courses but only as a total number of attendees for a course. No personal information on state and local law enforcement officials will be collected by DEA.

1.2 From whom is the information collected?

Learner information (name, work address, etc. as described above) for ATF, DEA and JMD employees, contractors and task force officers is obtained through a non-synchronous integration with the

Components' respective Human Resources application (HRConnect for ATF or National Finance Center for learnDOJ and DEALS) and the Global Address Locator (GAL). See **Appendix E** for the DOJ/OPM Data Feed Design.

For ATF, the HR Connect data is updated automatically Monday through Friday of every week. LearnATF external learner data is obtained from training application forms submitted by students, primarily on ATF E-Form 6400.1 State and Local Training Registration Request, ATF F 6330.1 Application for National Firearms Examiner Academy, or from sign-in sheets used at the training event (e.g. Project Safe Neighborhood). LMS administrator data is taken from e-Request records (see Section 8.4) submitted by Training Coordinators and Training Specialists. Employee instructor data is taken from the ATF Employee Instructor Application Form ATF F 6140.2 which is completed and submitted by instructors. Contract instructor data is collected as part of the contractual bidding process. Other Federal, state, or local volunteer instructor data is collected by the training manager responsible for the training event.

The employee learner data for learnDOJ and DEALS is manually downloaded from the National Finance Center (NFC) through a secure report and transferred via Secure File Transfer Protocol (SFTP) to a data center operated by Chief Information Office Operations Support Staff located on DOJ servers where it is processed to remove the first five digits of the SSN prior to being transferred to the LMS. The remaining four digits of SSN are combined with user first initial, middle initial and first four digits of the last name to create a unique user ID. Data for contractor learners is taken from the Global Address List (GAL). DEALS and learnDOJ Administrator data is taken from e-mail requests for administration accounts.

JMD manually collects instructor data from the staff sponsoring the training when the training item is set up in the LMS. DEA will manually collect instructor data from the Office of Training; in addition unique identifiers will be created for each instructor using information unique to their profile.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

The application captures the information necessary to uniquely identify each user and the DOJ-sponsored training they are required to take, have requested and/or have completed. OPM policy also requires the collection and reporting of training data for all Federal employees. The data required to be reported is listed in the OPM Guide to Human Resources Reporting and is outlined in **Appendix F**. In addition, maintaining detailed information about the training offered by DOJ/DEA/ATF and/or attended by DOJ/DEA/ATF personnel is necessary to respond to Bureau, Department and Government training information requests, reporting requirements and to measure human resource development program

effectiveness. Summary data from the LMS is used to track specific measures outlined in the Department of Justice Human Capital Strategic Plan. Data on RNO is collected to meet obligations under EEOC Management Directive 715 and RNO and gender information also is captured to fulfill ATF's obligations under the ATF African American Special Agent Class Action settlement. User data such as promotion date and entry on position are used to identify groups of individuals with specific training requirements to facilitate assignment of curricula. Certain mandatory training information is tracked for professional development purposes. No personal information from this system will be used for performance management functions.

Instructor data is collected by DOJ and ATF (and in the future, DEA) to identify instructors, assign them to scheduled offerings, and track instructor utilization. Administrator data is collected by DOJ/DEA/ATF to identify administrators, track their roles, and review their use of the LMS.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

General authority to collect the information in this system is 44 U.S.C. § 3101. Training information is collected and maintained under the provisions of the Government Employee Training Act (GETA), as codified in 5 U.S.C. §§ 4101-4118, with accompanying regulations promulgated in 5 C.F.R. § 410.311. Executive Order 11348, as amended by Executive Order 12107 also provides general authority for the collection of training information. Training data collected also is consistent with the Office of Personnel Management's Guide to Personnel Recordkeeping and Guide to Human Resources Reporting pursuant to 5 C.F.R. § 410.601. Collection of RNO information is also authorized by EEOC Management Directive 715. Certain online trainings are required to be completed by the Federal Information Security Management Act, 44 U.S.C. § 3541 et seq. Also, collection of data from ATF external learners on ATF F 6400.1, Training Registration Request for Non-ATF Students (OMB 1140-0053) and ATF F 6330.1, Application for National Firearms Examiner Academy (OMB 1140-0049) is authorized by OMB in accordance with the Paperwork Reduction Act of 1995.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The privacy risks are that the data might be compromised through unauthorized access to the LMS. The first mitigation factor is that the majority of the collected information that is maintained in the LMS is either available internally to other DOJ employees (through the GAL) or would be disclosed to the public pursuant to a FOIA request. Only a minimal amount of data in the system would not be considered public information (e.g., the four digits of the SSN and promotion dates).

The DOJ LMS Architecture has implemented a domain structure and domain restrictions that limit LMS administrators' ability to see learner data based on an established functional need. In addition, a privacy table is used to store specific sensitive learner data (gender and race national origin for LearnATF) in the LMS so that it is available for back-end reporting, but is not visible through the application interface. To further mitigate the risk of releasing privacy information, the LMS also

automatically limits supervisors' view and reporting privileges to only those learners that fall beneath them in the chain of command. As a web-based application, all interaction and exchange of data is done through a secure site using 128-bit encryption. SFTP is used to push ATF personnel data between the ATF network and the LMS application on a nightly basis. SFTP is also used to pull personnel data from NFC on a biweekly basis for learnDOJ and DEALS. All LMS support personnel and LMS users (including support contractors) undergo required background checks prior to receiving access to the application or data. The LMS application and hosting facility also completed OPM's Information Systems C&A process prior to being placed into production.

The full SSN is not held in the LMS. DEA and JMD tested over 15,000 records with a variety of combinations of information to create unique log-in IDs. The only combination that yielded no duplicates was First Initial, Middle Initial, the first four letters in the last name and the last four digits of SSN. For learnATF, ATF does not use SSN as part of the user ID because ATF assigns an unique employee identification number to each employee when they start employment with ATF. This employee ID serves as the login ID for ATF's LMS users. Given that the full SSN is not contained in the LMS and the protections described above, this is an acceptable level of risk.

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

Internally, data in the LMS is used to manage registrations for training events, track training resource utilization, assign learning and track completion of learning. Training information is retained and may be used to support that certain training was offered or provided by the government. Certain records are tracked for professional development purposes. Also, LMS data is used to report compliance with Government, Department or component training requirements.

Periodically ATF management is asked to analyze training records to identify trends and or anomalies. Some of these requests relate to the fair and equitable consideration of ATF employee's requests for participation in training programs. To fulfill these requests and ensure conformance of its training programs to Equal Employment Opportunity requirements, ATF has elected to store codes identifying the Race and National Origin (RNO) and gender of ATF employees in the system. These values are maintained in a privacy table and are not accessible to LMS administrators through the application interface. Management requests for data including these values can only be extracted through custom queries executed by the System Administrator on the backend data base.

Information about instructors is used for scheduling instructors for training events and to track instructor utilization. Administrator information is used to unlock accounts, reset passwords and to change/remove administrator roles from accounts.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

The application does not engage in data mining.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

The application includes a number of technical data validation checks to ensure accuracy of administrator input. Learner data for employees, contractors and task force officers is uploaded periodically and, with the exception of the employee's supervisor and e-mail address, is not edited by LMS administrators. In addition, a number of audit reports have been developed to allow system administrators to check for data errors and/or omissions. Internal users have visibility to their information through the learner side of the application enabling them to verify and validate primary profile information and training event information maintained in the LMS for them.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

A records retention schedule was approved by NARA for LearnATF and LearnDOJ. For ATF, the disposition of records is: destroy/delete learner records 25 years after the learner separates from the organization; destroy/delete course data 25 years after superseded or obsolete; destroy/delete instructor data when no longer associated with an active course; and destroy/delete reports when superseded or obsolete. For JMD, the disposition of records is: destroy/delete learner records 10 years after the learner separates from the organization; destroy/delete course data 5 years after superseded or obsolete; destroy/delete instructor data when no longer associated with an active course; and destroy/delete reports when superseded or obsolete.

All DEA training records, including DEALS system data, are under DEA review for comprehensive scheduling updates. Some data in the DEALS system is currently being retained indefinitely due to court order.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Use of data maintained in the LMS is addressed in the Rules of Behavior for End Users (as published in the respective Learner Guides) and in the Rules of Behavior for LMS Administrators (as included in the LMS for Training Coordinators and Training Specialists Training Manual). The Rules of

Behavior and repercussions associated with violations of them are addressed during the in-person training provided to LMS administrators. All report output is marked by default as "SBU- Sensitive but Unclassified." Audit logs are maintained for all learner and administrator use of the application. All access is based on administrator roles with access restricted to specific domains and responsibilities. Roles for administrators are not created and access granted until Rules of Behavior are acknowledged by the respective administrators. Network activity is also monitored with a continuously monitoring intrusion detection system.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

Training data and statistics from the LMS are shared with the Justice Management Division. Training data associated with mandatory training such as Ethics, NoFear Act/Whistleblower, Information Security Awareness, Equal Employment Opportunity and OSHA also may be shared by the Key System Administrators, through the appropriate Component program office, with Department auditors or program offices tasked with validating compliance with these training requirements.

4.2 For each recipient component or office, what information is shared and for what purpose?

Mandatory training data shared includes learner name, learner organization, item title, completion date and completion status. Training and statistics shared with Justice Management Division include learner counts by type, courseware licensing information and LMS application and database design information. Course completion totals for employees in core series also is shared with Justice Management Division to gauge skill gap closure in identified competencies for certain occupations. Usually, this information is shared via e-mail with appropriate attachments. For learnDOJ and DEALS the user ID, which consists of user first name initial, middle name initial, first four digits of the last name and last four digits of the SSN is masked in reports. ATF does not mask user ID because SSN is not part of its user ID.

4.3 How is the information transmitted or disclosed?

Data is extracted and disclosed based on the nature of the request – individual transcripts or learning records in electronic format if the inquiry concerns a particular individual(s) or electronic

spreadsheets of data for multiple individuals if the nature of the request is broader and is intended to address broader program requirements.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Possible risks are unauthorized access and/or misuse of data. As stated above in Section 2.3, most information collected is traditionally information released pursuant to FOIA and is considered traditionally in the public domain under OPM regulations. Only the minimum amount of information needed to accomplish the purpose for which the information is collected. The information will only be shared with authorized users who have a legitimate need to know. All requests for training data from the Department are processed by a select group of LMS system administrators. These administrators ensure that only the minimum amount of data required to fulfill each request is extracted from the LMS and disclosed to the requesting party. Where possible, personally identifiable information (PII) is masked or not included in the information being shared. LMS system administrators will only process requests for information received through the appropriate Component program office or at the behest of the Assistant Director, Learning and Workforce Development, Human Resources Staff, Justice Management Division or Component equivalent for the respective Component domains. The potential risk for unauthorized disclosure/misuse is mitigated by:

- Limiting the number of authorized users and the data they may access;
- Providing initial and annual system security training;
- Limiting physical access to the system hardware; and
- Monitoring network activity with a continuously monitoring intrusion detection system.

Section 5.0
External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

Enterprise Human Resources Integration (EHRI) training data is reported for Federal employees on a monthly basis in accordance with the OPM Guide to Human Resources Reporting. This information is transmitted through a SFTP system in an encrypted format. The report is generated by the DOJ/ATF/DEA LMS and sent to a data processing point residing on DOJ owned and operated servers at

the DOJ Rockville site. The data from learnATF, learnDOJ and DEALS is combined with data from the National Finance Center necessary for the OPM report which includes full SSN and Date of Birth (DOB) for each user which is matched by user ID prior to sending to OPM. The data is then combined with other reports from BOP, EOUSA and FBI prior to encrypted transmission via SFTP to OPM.

In addition, under the terms of ATF's Memorandum of Understanding with the Federal Emergency Management Agency (FEMA), learner completions by job location of the National Incident Management Systems (NIMS) training developed by FEMA, but hosted and tracked for ATF employees on learnATF, are provided to FEMA on a monthly basis. ATF also may share information about ATF contractors with their parent employer.

5.2 What information is shared and for what purpose?

Appendix F lists the data fields for EHRI reporting. The only PII transmitted is the full SSN and date of birth of DOJ learners (employees only). The purpose of this information is to meet OPM requirements to develop a consolidated database for Federal employee training records.

ATF information provided to FEMA for the purpose of tracking completion of FEMA courses includes numbers of students, by course, by employee category, and geographic location (state or region) that complete the NIMS online training. This information is being provided under the terms of the ATF-FEMA MOU and will be used by FEMA to validate ATF's compliance with the Homeland Security Presidential Directive on the Management of Domestic Incidents (HSPD-5). Information about mandatory training required by for a contractor may be shared with a contractor's parent employer.

There is no external sharing of instructor or administrator data from the LMS.

5.3 How is the information transmitted or disclosed?

The EHRI information is transmitted through a Secure File Transfer Protocol (SFTP) system in an encrypted format.

Training statistics including the number of individuals by location (city, state) and employment category (employee vs. contractor) who have completed each of the NIMS courses are transmitted electronically to FEMA on a monthly basis via e-mail. No data that can uniquely identify an individual is included in this transmission. This data will be transmitted to FEMA as long as the NIMS courses remain on the LMS in an active status.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

None for EHRI data.

No data that could be used to associate training information with a specific individual is provided under the terms of the ATF-FEMA MOU. There are no agreements concerning data shared with a parent employer about contract employees.

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

OPM EHRI users are required to take FISMA-required security awareness training.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

No.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Training data shared outside the Department is required by regulation. Sharing with OPM creates the risk of unauthorized access to the information which includes Social Security Number. This risk is mitigated by the use of Secure File Transfer Protocol and data encryption. The OPM EHRI Program Management Office is responsible for ensuring an adequate level of protection and security is afforded to EHRI systems. These protections are accomplished through an appropriate mix of technical, administrative, and managerial security controls including written guidance.

For the ATF-FEMA sharing, no data that could be used to associate training information with a specific individual is provided under the terms of the ATF-FEMA MOU; therefore privacy risks are mitigated. Sharing of information with contractors' parent employers is limited to the employee's name and the training that they are required to take.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of 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?

OPM has published a government-wide System of Records Notice (SORN) that covers training records about federal employees (including contractors and volunteers) at 71 F.R. 35342 (June 19, 2006) (OPM/GOVT-1, General Personnel Records). OPM's PIA for the GoLearn LMS, signed on September 26, 2006, and published at http://www.opm.gov/privacy/PIAs/GP-Plateau-LMS.pdf, states that OPM/GOVT-1, General Personnel Records, covers the records in the GoLearn LMS. Individual SORNs have also been published by ATF and DEA to cover certain training records in their components (ATF-010, Training and Professional Development Record System, 68 F.R. 3562 (Jan. 24, 2003) and DEA-015, Training Files, 52 F.R. 47217 (Dec. 11, 1987)). Additionally, DOJ-002, Department of Justice (DOJ) Computer Systems Activity and Access Records, 64 F.R. 73585 (Dec. 30, 1999) covers the collection of administrator information for the purpose of assigning those persons accounts on the GoLearn system.

A Privacy Act notice also is included on the ATF forms used to collect data from external learners (ATF E-Form 6400.1, State and Local Training Registration Request, and ATF F 6330.1, Application for National Firearms Examiner Academy) and instructors (ATF Employee Instructor Application Form ATF F 6140.2). A link to the DOJ Privacy Policy also is included on the login page of the LMS administrator site and on the learnATF user login page (DEA and JMD are adding this information to their respective login pages) and can be viewed at http://www.usdoj.gov/privacy-file.htm.

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

The information is automatically collected from the National Finance Center (NFC) data base or Component equivalent. Individuals do not have an opportunity to decline to provide information. For ATF external learners, statements are included on ATF F 6400.1, Training Registration Request for Non-ATF Students and ATF F 6330.1, Application for National Firearms Examiner Academy indicating that disclosure of SSN is voluntary and identifying the effects of non-disclosure. Non-disclosure may result in denial of the request or the applicant not being registered for the requested program. For ATF instructors, ATF Employee Instructor Application Form ATF F 6140.2 does state that collection is voluntary, but that non-entry of information may result in individuals not being eligible to serve as an instructor.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

No, individuals do not have an opportunity to consent to particular uses of the information. However, training information for external learners is captured for internal purposes including management and administration of training requests and program reporting only. Disclosure of information on an individual to external organizations and/or individuals would only occur with the individual's consent or through routine uses established in the OPM government-wide or DOJ component-specific SORNs discussed in 6.1.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The risk of lack of notice to individuals about information being collected about them and the uses of that information is mitigated by the publication in the Federal Register of System of Records Notices, Privacy Act notices on forms used to collect data, and links to the DOJ privacy policy on login pages.

Section 7.0
Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Individuals (including instructors who are also learners) can view their Learner Profiles and Learning Histories through the LMS. Individuals seeking to amend their profile information can do so by working with the HR Specialist within their division to make the change in the respective Human Resources system, as this is the originating source for all learner data. The corrected information will automatically be corrected in the LMS upon the next periodic update from the Human Resources data system. Types of information that may need to be changed include last name, duty location, supervisor, job position, etc. If specific training information (history) contained within the LMS is found to be inaccurate, the learner can work with their division Training Coordinator or the appropriate Systems Administrator to correct it. System administrators within the respective Components are the only individuals allowed to amend/delete learning event (history) information.

For JMD, an instructor would contact the Program Manager sponsoring the training who would then contact the System Administrator who set up the training in the LMS. For ATF, the instructor would contact the training manager responsible for the program for which they were an instructor if they needed a report on training events they instructed and/or needed this data corrected. Access to or correction to instructor records (name, contact information, areas of expertise) would be made to the Learning Management Branch which manages the instructor program for ATF. DEA does not currently maintain information in DEALS about instructors. Once such information is included in DEALS, if any changes are needed, instructors will contact the Learning and Technologies Program Office. Only the Office of Training's designated administrators will be able to make any corrections or changes to instructor information.

Administrators can view their profile information in the LMS. For ATF, correction of administrator information would be handled by the Learning Technologies Branch (LTB) key system administrators through submission of a help desk ticket or by email to the LTB. For DEA, administrators would contact the Learning and Technologies Program Office. Only the Office of Training's designated administrators can make any corrections or changes to administrator information.

Contractors may view their profile information through the LMS. Contractors' information may be corrected only by Systems Administrators. For JMD, the contractor would contact the staff Point of Contact/Training Coordinator sponsoring the training who would then contact the JMD System Administrator. Only system administrators can make changes to contractor records within the LMS. Non-DEA personnel (contractors) who participate in DEA training programs should contact either the Learning Technologies Program Office or their division's Human Resource Coordinator to make any corrections to their personal information. Only the Office of Training's designated administrators can make any corrections or changes to the learning event/history of a non-DEA person.

ATF contractor records are maintained through the same mechanism used for employee data. Correction to profile data would therefore be made in the system of origin (HRConnect or Global Address Locator). Non-ATF personnel who participate in ATF training programs may contact the ATF office that sponsored the training requesting documentation or correction of their training records. Requests must be made in person or in writing. Prior to disclosure, validation of the individuals' identity will be made using available information on the applicable training record. Individual class completion certificates and/or learning history reports can be generated from the system to satisfy these requests. Incorrect data associated with an external learner's profile can be amended by the Training Specialists who manage the program the applicant has requested participation in. Inaccuracies in learning history can be researched using paper-based or imaged course files, and if found to be valid, can be corrected in the LMS by a system administrator.

Additionally, individuals can seek access and amendment under the Privacy Act as provided for in the appropriate SORNs.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Instructions for changing information on the learner profile are included in the Learner Guide. This guide was distributed to all employees at the time the LMS was launched and also is available electronically on the Intranet. Help Desk technicians also have been advised to instruct users on the process for correcting profile data. DOJ/DEA Employees are advised that the procedure for changing information regarding their e-mail address and/or supervisor is to contact their Training Coordinators. DOJ/DEA employees are advised to contact their servicing personnel representative to change other information because it requires correction within the National Finance Center database.

For ATF, most external learners receive certificates upon training completion that reflect the event data that will be entered in their Learning History. They can request amendment of the information at that time through the Training Specialist managing the training. Access to the information at a later date would be through ATF's standard process for Privacy Act requests.

Procedures for making access and amendment requests under the Privacy Act may be found in the appropriate SORNs.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

The opportunity to amend information is provided as described above.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

Opportunities for contesting information in the LMS are described above in Section 7.2. No actions are taken as a result of agency reliance on information in the LMS for external learners. The only action taken based on agency reliance on information in the LMS for personnel is possible repercussions for non-completion of mandatory training. Individuals who wish to contest information in the LMS concerning their fulfillment of mandatory training requirements can do so by contacting the appropriate Training Specialist, division Training Coordinator or Component Key System Administrator.

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

The following user groups have access to the administrative functions of the LMS.

- Key System Administrators – Staff within the respective Components who manage the configuration, daily operation, data integrity and security of the application.
- Curriculum Managers – Staff within the ATF Learning Systems Management Division that maintain and edit Item, Curricula, and Instructor records.
- Training Specialists – Staff within the ATF Office of Training and Professional Development that have view and/or limited edit rights within the application.
- Training Coordinators – Staff within the respective Components' directorates/divisions that are responsible for managing training registrations, assisting management with training approvals, recording division-based and external training event completions and reporting on the training completed and required by employees within their directorates/divisions.
- Contractors – Contractors who have successfully passed a background investigation and who are responsible for maintaining the LMS operating environment and providing Help Desk support for the LMS.
- Human Resource Coordinators (HRC) – DEA Staff within the administration who are responsible for managing and updating employee supervisor information.
- Computer Security Awareness Training (CSAT) Administrators – Staff within the respective Components directorates/divisions that are responsible for managing completion of the CSAT program.

The following user groups have access to the learner functions of the LMS:

- Employees
- Contractors (including users of the National Integrated Ballistics Information Network) required to complete one or more of DOJ's mandatory training courses.
- ATF Task Force Officers required to complete one or more of ATF's mandatory training courses.
- DEA Task Force Officers who supervise DEA employees.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

All DOJ contractors and task force officers with access to LMS information systems and facilities are required to take online mandatory training under the requirements established in the Federal Information Security Management Act. They are therefore automatically granted access to the learner-related functions of the LMS for this purpose.

Contractors hired to assist with the maintenance, operation and support of the LMS have access to administrative functions under the terms of the contract issued to them by the Office of Personnel Management's GoLearn program (under a reimbursable agreement with DOJ). For ATF, the contract that defines the role of contractors providing Help Desk support for the LMS is the same as the one issued by ATF's Office of Science and Technology to acquire similar services for other ATF applications.

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

Roles are used within the LMS to assign administrator privileges. Users can be granted one or more administrator roles. Roles consist of one or more workflows that allow administrators to perform job relevant functions within the LMS. Roles are further limited by domain and entity restrictions. Domain restrictions applied to role definitions limit administrator view and edit privileges to only those records in the LMS for which the user has a bona fide need. Roles also are used to define user access to functions. Roles are defined by LMS administrators and assigned automatically to new learner accounts based on pre-established assignment profiles.

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

For learnDOJ and DEALS, all employees and contractors are automatically provided access to the LMS learner site upon creation of a record for them in the National Finance Center or Global Address Locator data bases. Administrator accounts are created on an as needed basis. Individuals must complete and provide a completed additional Rules of Behavior (ROB) for administrators. Component Training Coordinators must provide the signed ROB to their respective Component Key System Administrator. Component Key System Administrators must provide signed ROB to the JMD Key System Administrator.

For ATF, all ATF employees, contractors and task force officers are automatically provided access to the LMS learner site upon the creation of a record for them in HRConnect and the ATF Global Address Locator. This process is documented on the ATF Intraweb and in the learnATF Administrator Guides. ATF Administrator accounts are created on an as needed basis. Individuals must submit an e-Request for system access along with a signed copy of the LMS Administrator Rules of Behavior before access is provided. These requests must be approved by the employee's supervisor. Upon receipt of the e-Request, the ATF LMS System Owner authorizes creation of an administrator account. This process is

documented in office Standard Operating Procedures LTB-00 and LTB-009 and described on the ATF Intraweb.

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

Roles for ATF are specified on the e-Request and approved by the employee's supervisor and the LMS System Owner prior to account creation. Audit logs are maintained for all administrator access to the site to verify activities conducted are commensurate with assigned roles.

Roles will be specified on the signed DEALS Administration account request form for access to DEALS. The form is reviewed and approved by the employee's supervisor and the Office of Training prior to the creation of the account. This process will be documented in the DEALS user manual. Furthermore, DEALS employs tracking and audit logs that can monitor the activities of any particular user. The system uses role-based access controls and restricts data by user classification.

Roles for administrative access to learnDOJ are documented by e-mail from the respective Component's Key System Administrator and kept on file. Roles are not created and access granted until a signed Rules of Behavior form is received from the individual being assigned the role/access.

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

Technical safeguards to prevent misuse of data maintained in the LMS include workflow and domain restrictions associated with every administrator account, automatic labeling of all system output as Sensitive But Unclassified, Rules of Behavior established for both learner and administrative users of the application and audit capabilities/reports in the application. Physical access is limited to key system hardware. Background checks are performed on all systems support personnel. Network activity is monitored with a continuously monitoring intrusion detection system.

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

All administrative users of the application are required to read and sign the LMS Administrator Rules of Behavior prior to receiving system access. These are found within the LMS Administrator Guide each administrator receives upon requesting access to the application. The Rules of Behavior contain information about maintaining sensitive data and discuss the users' responsibilities associated with securing the data maintained in the application. The Rules of Behavior also are covered during the in-person training provided to LMS administrators.

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

Data is secured in accordance with FISMA requirements. A C&A, dated February 8, 2007, for the LMS is on file with the OPM Security Officer. This C&A is updated as required as system changes are made.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Numerous technical and operational controls are in place in the application and have been documented in the LMS Security Plan. These controls mitigate privacy risks associated with the unauthorized access to and use of the data maintained. Also see the discussion in Section 3.5.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

DOJ evaluated several commercial LMS products to determine the product best suited to meet the Department's needs. The three major legacy LMS operating with DOJ were evaluated for expansion. All DOJ Components not having employees covered by a legacy LMS were given the choice of selecting either the LMS operated by the Executive Office of U.S. Attorneys, JUSTLearn, or the LMS operated by ATF as that Component's LMS. JMD and DEA chose to be included under the expanded ATF LMS. The ATF LMS was chosen for expansion because it was contracted through an OPM-approved Customer Service Provider in accordance with the Presidential Management Agenda Human Resources/Human Resources Development Line of Business in accordance with Office of Management and Budget and OPM policies. ATF selected the Plateau LMS after evaluating several commercial-off-the-shelf products available under the OPM/GoLearn vehicle against an established set of functional requirements.

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

Security features of the application including the ability to control access to data were analyzed. The LMS product selected (Plateau) best met the requirements for managing data integrity, privacy and

security through its ability to easily configure domains/roles at a granular level and its extensive auditing of system transactions.

9.3 What design choices were made to enhance privacy?

Decisions on the configuration of roles and domains in the LMS were made so as to restrict administrator access to the lowest level possible given each administrator's functional needs and responsibilities. All reports produced are considered and are labeled "Sensitive But Unclassified – SBU." The Plateau LMS was customized to include the "Government System Warning" message as users sign-in. For learnATF a privacy table was created for highly sensitive data about learners (e.g. gender, RNO) and to prevent access to the data through the application interface. In deciding on a user log-in, JMD and DEA tested over 15,000 records with a variety of combinations of information to create unique log-ins. The only combination that yielded no duplicates was First Initial, Middle Initial, the first four letters in the last name and the last four digits of SSN. Given that the full SSN is not contained in the LMS, this is an acceptable level of risk. ATF was able to utilize a log-in that did not contain SSNs because ATF assigns a unique employee identification number to each employee when they start employment with ATF. This employee ID serves as the login ID for ATF's LMS users. Secure Socket Layer (SSL) encryption was added to the system to protect data in transmission and password configuration settings were set based on applicable NIST requirements.

Conclusion

Privacy risks associated with the LMS (Plateau) are mitigated by minimizing the information collected to the minimum amount needed to accomplish the functions of the system. In addition, most of the personal information that is collected is available internally to other DOJ employees in Outlook or would be released to the public in a FOIA request. For the few elements of data that are not readily available, a privacy table hides those elements of sensitive privacy data in the LMS from most users. Moreover, the LMS (Plateau) was selected in part based on an assessment of its inherent technical security controls. These controls, which are easily configured, allow system administrators to determine and control which functions administrators should have access to and which records administrators should be able to view at a very granular level. Extensive auditing capabilities inherent to the application also help mitigate privacy risks. Access control policies and procedures developed for the application ensure that only individuals with a bona fide need to access training data are granted administrative privileges. Sharing of information from the LMS is only to those who have a legitimate need for the information based on their assigned job roles and/or responsibilities. All of these features ensure the protection of the information provided by learners, instructors and administrators of the LMS.

Responsible Officials

learnATF
Wendy L. Frederick

Learning Systems Management Division
Office of Training and Professional Development
Bureau of Alcohol, Tobacco, Firearms and Explosives
202-648-8397

DEALS
Michele R. Norris
Learning Technologies Program Manager
Office of Training
Drug Enforcement Administration
703-632-5159

learnDOJ
Al Stiles
Enterprise Learning Technologies Program Officer
Justice Management Division/Human Resources Staff
Department of Justice
(202) 353-1605

Approval Signature Page

/s/ 5/21/10

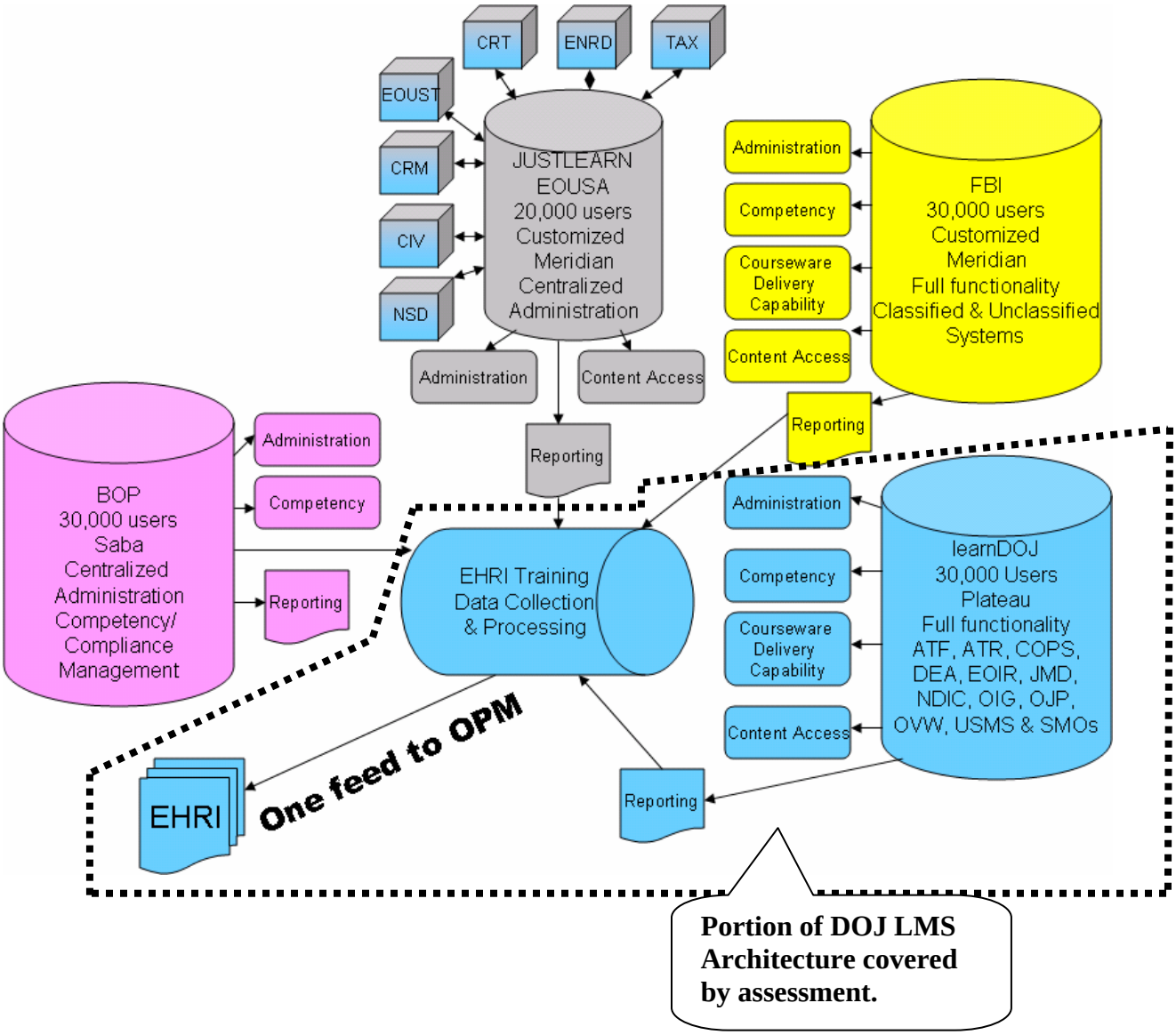
Mari Barr Santangelo Date
Deputy Assistant Attorney General for Human Resources Administration
Department of Justice

/s/ 5/3/10

Nancy C. Libin Date
Chief Privacy and Civil Liberties Officer
Department of Justice

Appendix A

Department Of Justice Learning Management System Architecture



Appendix B– ATF Data Tables for Learner, Instructor and Administrator

User Data

Plateau Field	Description	ATF Employee	ATF Contractor/TFO	External Learner
Last Name	The user's last name	x	x	x
First Name	The user's first name and Middle Initial	x	x	x
Job Title	The user's job descriptive job title.	x	x	x
Job Position	The user's job position description.	x	x	
Job Location	Code representing the city, state and zip code of the user's work location or for external users ATF Field Division user is associated with.	x	x	x
Domain	Code identifying domain assignment for user which determines visibility to record by administrators.	x	x	x
Role	Code identifying self-service access rights provided to user.	x	x	x
Organization	The user's organization code or 999999 for externals.	x	x	x
Employee Type	Code indicating if user is supervisory, non-supervisory, contractor or external user.	x	x	x
Employee Status	User's employment status (e.g. full-time, part-time, intermittent)	x	x	
Address	The user's work address.	x	x	x
City	The user's work city.	x	x	x
County	The County	x	x	
State/Province	The state where the user's work location is located.	x	x	x
PostalCode	The zip code, APO, Foreign Zip Code where the user's work location is located. Should be set to N/A if foreign zip or APO is used.	x	x	x
Country	The user's work country.	x	x	x
Email Address	The user's email address used to send notifications to the user.	x	x	x
Hired	Entry on Duty, the start date of the user for his/her current agency.	x		
Terminated	The last day of employment at the organization for the user. Will drive value for Active field.	x	x	
Supervisor	Supervisor's User ID	x	x	
Phone/Fax Number	The user's work phone and/or fax numbers.	x	x	x

Plateau Field	Description	ATF Employee	ATF Contractor/TFO	External Learner
Branch of Government	Branch of Federal Government user works for.	x	x	
Federal Department	Federal Government Department that user works for.	x	x	
Agency/Bureau	Agency or Bureau within the Department specified that the user works for.	x	x	
Directorate/External Department	Directorate within Agency or Bureau that user works for or in the case of external users the organization the user works for (e.g. Los Angeles County Sheriff's Office)	x	x	x
Division	Division within Directorate that user works for.	x	x	
Branch	Branch within Division that user works for.	x	x	
Last Four SSN	Last four-digits of user's SSN.	x	x	x
Employee Type	Indicates whether user is a supervisor, a non-supervisory employee, a contractor, task force officer or for external users the level of Government the individual works for (e.g. State, local, tribal, Federal civilian or Federal military)	x	x	x
Employee Number	The user's unique employee number or id from the HR system of record	x	x	
Pay Plan	The user's pay plan. For example, GS, SES, etc.	x		
Job Series	The user's job series. All 0000 for non-employees.	x		
Pay Grade	The user's pay grade. Usually a numerical identifier.	x		
Step	The user's step on the pay grade scale.	x		
Education Level	The highest level of education attained by the user.	x	x	
Clearance Level	The level of security clearance attained by the user.	x	x	
Master Position Number	The number of the position to which the user is assigned.	x	x	
Appointment Type	The type of appointment under which the user is serving.	x		
2nd Level Supervisor	User ID of employee's supervisor's supervisor	x	x	
Training Coordinator	ID of user who serves as the Training Coordinator for the user's division	x	x	
Contractor Name	If user is a contractor, name of employing company.		x	

Plateau Field	Description	ATF Employee	ATF Contractor/TFO	External Learner
Non-DOJ Supervisor Name	Supervisor's Full Name (First and Last) if not a DOJ employee			x
Fire Department	For external users employed by a Fire Department (Y or N)			x
Non-DOJ Supervisor Phone	Phone number of external user's supervisor			x
Non-DOJ Supervisor E-mail	E-mail address of external user's supervisor			x
Dog Microchip Number	If user is a canine or canine handler, microchip number of dog	x		x
ID in Migrated System	The user's ID in the system the user's data is coming from.	x	x	
System Migrated From	System from which the user's HR data was taken from.	x	x	
Master Record Number	Unique record number associated with user in system from which data has been taken.	x	x	
Continuing Service Agreement	Indicates whether user is serving under a continuing service agreement.	x		
Continuing Service Agreement End Date	If user is serving under a CSA, date the CSA ends.	x		
LMS Create Date	Date user's record was created in the system.	x	x	x
New Account	Indicates if user's record was created within the last 30 days.	x	x	x
Rules of Behavior	If user is a system administrator, indicator of whether they have signed the Rules of Behavior for system use.	x	x	
E-Request Processed	If user is a system administrator, indicator of whether they have submitted official request for system access.	x	x	
EHRI ID	Unique ID assigned to user in DOJ EHRI database to allow matching to SSN and birth date for EHRI submissions.	x		
POI	Personnel Office Indicator for user's organization	x	x	
OPM Organization ID	OPM ID assigned to user's organization	x	x	
County	County of user's job location	x	x	
Entry on Service	Start date of the user for government employment.	x		
Entry on Position	Date the user entered into his/her current job position.	x		

Plateau Field	Description	ATF Employee	ATF Contractor/TFO	External Learner
Entry on Management	If the user is a supervisor, date that he/she first entered a supervisory position in organization.	x		
Promotion Date	The user's most recent promotion date.	x		
Gender	(Maintained in a Privacy Table as encrypted data – not visible through system interface) The user's gender. Used for statistical reporting.	x	x	
RNO	(Maintained in a Privacy Table – not visible through system interface) The user's race or national orgin. Used for statistical reporting.	x		
Salary	(Maintained in a Privacy Table – not visible through system interface) The user's salary. Used to determine training costs.	x		

Instructor Data

Plateau Field	Description	Employee	Contractor
Last Name	The instructor's last name	x	x
First Name	The instructor's first name and Middle Initial	x	x
Company	The instructor's company or for internal instructors the division and field office the instructor is assigned to.	x	x
Domain	Code identifying domain assignment for instructor which determines visibility to record by administrators.	x	x
Organization	The instructor's Organization ID	x	x
Email Address	The instructor's email address used to send notifications.	x	x
Comments	For contract instructors may include rates and information concerning when the instructor successfully passed a background investigation.		x
Address	The instructor's work address.	x	x
City	The instructor's work city.	x	x
State	The state where the instructor's work location is located.	x	x
PostalCode	The zip code, APO, Foreign Zip Code where the instructor's work location is located. Should be set to N/A if foreign zip or APO is used.	x	x
Country	The instructor's work country.	x	x
Telephone	The instructor's work phone number.	x	x

Plateau Field	Description	Employee	Contractor
Fax	The instructor's fax number	x	x
Contract #	If a contract instructor, the number of the contract the instructor is authorized to instruct under.		x
Contract Date	If a contract instructor, the date the contract the instructor is authorized to instruct under was issued.		x
Contract Expiration Date	If a contract instructor, the date the contract the instructor is authorized to instruct under expires.		x
Application Date	Date instructor submitted application to become an instructor.	x	
Verification Date	Date experience/expertise included on application was verified.	x	
Certification Date	Date instructor was certified to instruct.	x	
Education/Experience	Education/experience that relates to instructor's ability to instruct in a particular subject area.	x	x
Job Series	The instructor's Job Series	x	
SME Designation	Subject areas in which instructor is authorized to teach.	x	x

Administrator Data

Plateau Field	Description	Sample Value
Last Name	The administrator's last name	Smith
First Name	The administrator's first name and Middle Initial	James E
Domain	Code identifying domain assignment for instructor which determines visibility to record by administrators.	ADMINISTRATION
Email Address	The administrator's email address used to send notifications.	james.smith@atf.gov

Appendix C – learnDOJ Data Tables for Learner, Instructor and Administrator

User Data

Plateau Field	Description	DOJ Employee	DOJ Contractor
Last Name	The user's last name	x	x
First Name	The user's first name and Middle Initial	x	x
Job Title	The user's job descriptive job title.	x	x
Job Position	The user's job position description.	x	x
Job Location	Code representing the city, state and zip code of the user's work.	x	x
Domain	Code identifying domain assignment for user which determines visibility to record by administrators.	x	x
Role	Code identifying self-service access rights provided to user.	x	x
Organization	The user's organization code or 999999 for externals.	x	x
Employee Type	Code indicating if user is supervisory, non-supervisory, contractor or external user.	x	x
Employee Status	User's employment status (e.g. full-time, part-time, intermittent)	x	x
Address	The user's work address.	x	x
City	The user's work city.	x	x
County	The County	x	x
State/Province	The state where the user's work location is located.	x	x
PostalCode	The zip code, APO, Foreign Zip Code where the user's work location is located. Should be set to N/A if foreign zip or APO is used.	x	x
Country	The user's work country.	x	x
Email Address	The user's email address used to send notifications to the user.	x	x
Hired	Entry on Duty, the start date of the user for his/her current agency.	x	
Terminated	The last day of employment at the organization for the user. Will drive value for Active field.	x	x
Supervisor	Supervisor's User ID	x	x
Phone/Fax Number	The user's work phone and/or fax numbers.	x	x
Branch of Government	Branch of Federal Government user works for.	x	x

Plateau Field	Description	DOJ Employee	DOJ Contractor
Federal Department	Federal Government Department that user works for.	x	x
Agency/Bureau	Agency or Bureau within the Department specified that the user works for.	x	x
Directorate/External Department	Directorate within Agency or Bureau that user works for or in the case of external users the organization the user works for (e.g. Los Angeles County Sheriff's Office)	x	x
Division	Division within Directorate that user works for.	x	x
Branch	Branch within Division that user works for.	x	x
Last Four SSN	Last four-digits of user's SSN.	x	x
Employee Type	Indicates whether user is a supervisor, a non-supervisory employee, a contractor, task force officer or for external users the level of Government the individual works for (e.g. State, local, tribal, Federal civilian or Federal military)	x	x
Employee Number	The user's unique employee number or id from the HR system of record		
Pay Plan	The user's pay plan. For example, GS, SES, etc.	x	x
Job Series	The user's job series. All 0000 for non-employees.	x	x
Pay Grade	The user's pay grade. Usually a numerical identifier.	x	
Step	The user's step on the pay grade scale.	x	
Education Level	The highest level of education attained by the user.	x	x
Clearance Level	The level of security clearance attained by the user.	x	x
Master Position Number	The number of the position to which the user is assigned.	x	x
Appointment Type	The type of appointment under which the user is serving.	x	x
2nd Level Supervisor	User ID of employee's supervisor's supervisor	x	x
Training Coordinator	ID of user who serves as the Training Coordinator for the user's division	x	x
Contractor Name	If user is a contractor, name of employing company.		x
Non-DOJ Supervisor Name	Supervisor's Full Name (First and Last) if not a DOJ		

Plateau Field	Description	DOJ Employee	DOJ Contractor
	employee		
Fire Department	For external users employed by a Fire Department (Y or N)		
Non-DOJ Supervisor Phone	Phone number of external user's supervisor		
Non-DOJ Supervisor E-mail	E-mail address of external user's supervisor		
Dog Microchip Number	If user is a canine or canine handler, microchip number of dog	x	
ID in Migrated System	The user's ID in the system the user's data is coming from.	x	x
System Migrated From	System from which the user's HR data was taken from.	x	x
Master Record Number	Unique record number associated with user in system from which data has been taken.	x	x
Continuing Service Agreement	Indicates whether user is serving under a continuing service agreement.	x	
Continuing Service Agreement End Date	If user is serving under a CSA, date the CSA ends.	x	
LMS Create Date	Date user's record was created in the system.	x	x
New Account	Indicates if user's record was created within the last 30 days.	x	x
Rules of Behavior	If user is a system administrator, indicator of whether they have signed the Rules of Behavior for system use.	x	x
E-Request Processed	If user is a system administrator, indicator of whether they have submitted official request for system access.	x	x
EHRI ID	Unique ID assigned to user in DOJ EHRI database to allow matching to SSN and birth date for EHRI submissions.	x	
POI	Personnel Office Indicator for user's organization	x	x
OPM Organization ID	OPM ID assigned to user's organization	x	x
County	County of user's job location	x	x
Entry on Service	Start date of the user for government employment.	x	x
Entry on Position	Date the user entered into his/her current job position.	x	
Entry on Management	If the user is a supervisor, date that he/she first entered a supervisory position in	x	

Plateau Field	Description	DOJ Employee	DOJ Contractor
	organization.		
Promotion Date	The user's most recent promotion date.	x	

Instructor Data

Plateau Field	Description	Employee	Contractor
Last Name	The instructor's last name	x	x
First Name	The instructor's first name and Middle Initial	x	x
Company	The instructor's company or for internal instructors the division and field office the instructor is assigned to.	x	x
Domain	Code identifying domain assignment for instructor which determines visibility to record by administrators.	x	x
Organization	The instructor's Organization ID	x	x
Email Address	The instructor's email address used to send notifications.	x	x
Comments	For contract instructors may include rates and information concerning when the instructor successfully passed a background investigation.		x
Address	The instructor's work address.	x	x
City	The instructor's work city.	x	x
State	The state where the instructor's work location is located.	x	x
PostalCode	The zip code, APO, Foreign Zip Code where the instructor's work location is located. Should be set to N/A if foreign zip or APO is used.	x	x
Country	The instructor's work country.	x	x
Telephone	The instructor's work phone number.	x	x
Fax	The instructor's fax number	x	x
Contract #	If a contract instructor, the number of the contract the instructor is authorized to instruct under.		x
Contract Date	If a contract instructor, the date the contract the instructor is authorized to instruct under was issued.		x
Contract Expiration Date	If a contract instructor, the date the contract the instructor is authorized to instruct under expires.		x
Application Date	Date instructor submitted application to become an instructor.	x	
Verification Date	Date experience/expertise included on application was verified.	x	
Certification Date	Date instructor was certified to instruct.	x	
Education/Experience	Education/experience that relates to instructor's	x	x

	ability to instruct in a particular subject area.		
Job Series	The instructor's Job Series	x	
SME Designation	Subject areas in which instructor is authorized to teach.	x	x

Administrator Data

Plateau Field	Description	Sample Value
Last Name	The administrator's last name	Smith
First Name	The administrator's first name and Middle Initial	James E
Domain	Code identifying domain assignment for instructor which determines visibility to record by administrators.	ADMINISTRATION
Email Address	The administrator's email address used to send notifications.	james.smith@usdoj.gov

Appendix D – DEALS Data Tables for Learner, Instructor and Administrator

User Data

Plateau Field	Description	DOJ Employee	DOJ Contractor
Last Name	The user's last name	x	x
First Name	The user's first name and Middle Initial	x	x
Job Title	The user's job descriptive job title.	x	x
Job Position	The user's job position description.	x	x
Job Location	Code representing the city, state and zip code of the user's work.	x	x
Domain	Code identifying domain assignment for user which determines visibility to record by administrators.	x	x
Role	Code identifying self-service access rights provided to user.	x	x
Organization	The user's organization code or 999999 for externals.	x	x
Employee Type	Code indicating if user is supervisory, non-supervisory, contractor or external user.	x	x
Employee Status	User's employment status (e.g. full-time, part-time, intermittent)	x	x
Address	The user's work address.	x	x
City	The user's work city.	x	x
County	The County	x	x
State/Province	The state where the user's work location is located.	x	x
PostalCode	The zip code, APO, Foreign Zip Code where the user's work location is located. Should be set to N/A if foreign zip or APO is used.	x	x
Country	The user's work country.	x	x
Email Address	The user's email address used to send notifications to the user.	x	x
Hired	Entry on Duty, the start date of the user for his/her current agency.	x	
Terminated	The last day of employment at the organization for the user. Will drive value for Active field.	x	x
Supervisor	Supervisor's User ID	x	x
Phone/Fax Number	The user's work phone and/or fax numbers.	x	x
Branch of Government	Branch of Federal Government user works for.	x	x

Plateau Field	Description	DOJ Employee	DOJ Contractor
Federal Department	Federal Government Department that user works for.	x	x
Agency/Bureau	Agency or Bureau within the Department specified that the user works for.	x	x
Directorate/External Department	Directorate within Agency or Bureau that user works for or in the case of external users the organization the user works for (e.g. Los Angeles County Sheriff's Office)	x	x
Division	Division within Directorate that user works for.	x	x
Branch	Branch within Division that user works for.	x	x
Last Four SSN	Last four-digits of user's SSN.	x	x
Employee Type	Indicates whether user is a supervisor, a non-supervisory employee, a contractor, task force officer or for external users the level of Government the individual works for (e.g. State, local, tribal, Federal civilian or Federal military)	x	x
Employee Number	The user's unique employee number or id from the HR system of record		
Pay Plan	The user's pay plan. For example, GS, SES, etc.	x	x
Job Series	The user's job series. All 0000 for non-employees.	x	x
Pay Grade	The user's pay grade. Usually a numerical identifier.	x	
Step	The user's step on the pay grade scale.	x	
Education Level	The highest level of education attained by the user.	x	x
Clearance Level	The level of security clearance attained by the user.	x	x
Master Position Number	The number of the position to which the user is assigned.	x	x
Appointment Type	The type of appointment under which the user is serving.	x	x
2nd Level Supervisor	User ID of employee's supervisor's supervisor	x	x
Training Coordinator	ID of user who serves as the Training Coordinator for the user's division	x	x
Contractor Name	If user is a contractor, name of employing company.		x
Non-DOJ Supervisor Name	Supervisor's Full Name (First and Last) if not a DOJ		

Plateau Field	Description	DOJ Employee	DOJ Contractor
	employee		
Fire Department	For external users employed by a Fire Department (Y or N)		
Non-DOJ Supervisor Phone	Phone number of external user's supervisor		
Non-DOJ Supervisor E-mail	E-mail address of external user's supervisor		
Dog Microchip Number	If user is a canine or canine handler, microchip number of dog	x	
ID in Migrated System	The user's ID in the system the user's data is coming from.	x	x
System Migrated From	System from which the user's HR data was taken from.	x	x
Master Record Number	Unique record number associated with user in system from which data has been taken.	x	x
Continuing Service Agreement	Indicates whether user is serving under a continuing service agreement.	x	
Continuing Service Agreement End Date	If user is serving under a CSA, date the CSA ends.	x	
LMS Create Date	Date user's record was created in the system.	x	x
New Account	Indicates if user's record was created within the last 30 days.	x	x
Rules of Behavior	If user is a system administrator, indicator of whether they have signed the Rules of Behavior for system use.	x	x
E-Request Processed	If user is a system administrator, indicator of whether they have submitted official request for system access.	x	x
EHRI ID	Unique ID assigned to user in DOJ EHRI database to allow matching to SSN and birth date for EHRI submissions.	x	
POI	Personnel Office Indicator for user's organization	x	x
OPM Organization ID	OPM ID assigned to user's organization	x	x
County	County of user's job location	x	x
Entry on Service	Start date of the user for government employment.	x	x
Entry on Position	Date the user entered into his/her current job position.	x	
Entry on Management	If the user is a supervisor, date that he/she first entered a supervisory position in	x	

Plateau Field	Description	DOJ Employee	DOJ Contractor
	organization.		
Promotion Date	The user's most recent promotion date.	x	

Instructor Data

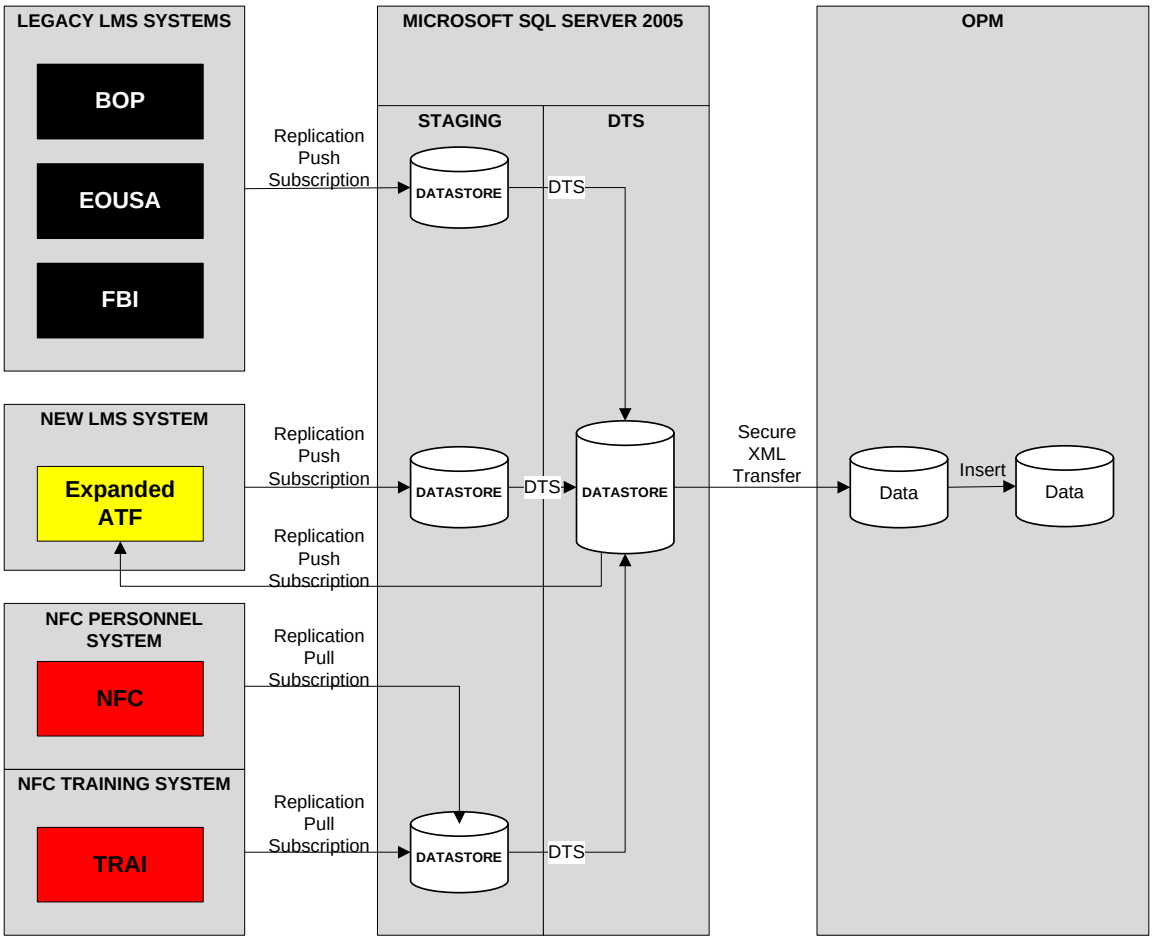
Plateau Field	Description	Employee	Contractor
Last Name	The instructor's last name	x	x
First Name	The instructor's first name and Middle Initial	x	x
Company	The instructor's company or for internal instructors the division and field office the instructor is assigned to.	x	x
Domain	Code identifying domain assignment for instructor which determines visibility to record by administrators.	x	x
Organization	The instructor's Organization ID	x	x
Email Address	The instructor's email address used to send notifications.	x	x
Comments	For contract instructors may include rates and information concerning when the instructor successfully passed a background investigation.		x
Address	The instructor's work address.	x	x
City	The instructor's work city.	x	x
State	The state where the instructor's work location is located.	x	x
PostalCode	The zip code, APO, Foreign Zip Code where the instructor's work location is located. Should be set to N/A if foreign zip or APO is used.	x	x
Country	The instructor's work country.	x	x
Telephone	The instructor's work phone number.	x	x
Fax	The instructor's fax number	x	x
Contract #	If a contract instructor, the number of the contract the instructor is authorized to instruct under.		x
Contract Date	If a contract instructor, the date the contract the instructor is authorized to instruct under was issued.		x
Contract Expiration Date	If a contract instructor, the date the contract the instructor is authorized to instruct under expires.		x
Application Date	Date instructor submitted application to become an instructor.	x	
Verification Date	Date experience/expertise included on application was verified.	x	
Certification Date	Date instructor was certified to instruct.	x	
Education/Experience	Education/experience that relates to instructor's	x	x

	ability to instruct in a particular subject area.		
Job Series	The instructor's Job Series	x	
SME Designation	Subject areas in which instructor is authorized to teach.	x	x

Administrator Data

Plateau Field	Description	Sample Value
Last Name	The administrator's last name	Smith
First Name	The administrator's first name and Middle Initial	James E
Domain	Code identifying domain assignment for instructor which determines visibility to record by administrators.	ADMINISTRATION
Email Address	The administrator's email address used to send notifications.	james.smith@usdoj.gov

Appendix E – DOJ/OPM Data Feed Design



Note:

1. Legacy Systems – BOP, EOUSA, and FBI will push EHRI training data to the Data Feed staging DataStore. (Components who do not have a LMS will use any of the Legacy LMSs or TRAI for the reporting of EHRI data)
    a. Some Legacy LMS Systems currently do not have or use all of the required EHRI data fields. This means the EHRI data fields will need to be created within the Legacy LMS's or the missing data will come from the TRAI system which house some DOJ HR data.
2. New LMS Systems – ATF, DEA, and JMD will use the expanded ATF (Plateau LMS). ATF's Plateau system will push EHRI training data to the Data Warehouse staging Data Store. The Data Feed will push user population updates to the “Expanded ATF” LMS using one-way encryption of the Social Security Account Number (SSAN) to create a unique identifier for each Federal Employee user. SSAN and Date of Birth information is deleted from the NFC data file before it is pushed from the DOJ datastore to the LMS.
3. Training Systems – TRAI, All EHRI data from TRAI will be pulled from TRAI to the Data Feed staging DataStore. (Components who do not have a LMS will use any of the Legacy LMSs or TRAI for the reporting of EHRI data).
4. NFC Personnel System – NFC personnel data from the NFC Personnel Action Data Base will be pulled from NFC to the Data Feed to maintain the user data base.
5. All EHRI data will be converted /consolidated into a single file within the Data Feed and sent to OPM.

Appendix F – OPM EHRI Data Fields

Chapter 4 of the OPM Guide to Human Resources Reporting contains specific information on the preparation and submission of training data files. Chapter 4 can be accessed at http://www.opm.gov/feddata/ghrr/ghrr07_ch4.pdf .

ICD Seq #	EHRI Ref #	Data Concept	Name	Datatype	Definition	Notes
1	997	Date Record	Record Action	VARCHAR (1)	Indicates action to take with this data record.	A=Add, D=Delete, C=Correct.
2	652	Employee ID	Social Security Number (SSN)	VARCHAR(35)	Person's Social Security Number.	
3	74	Employee ID	Birth Date	DATE	Date on which the person is born.	Used in combination with SSN to uniquely identify an employee.
4	999	Employee ID	EHRI Employee ID	NUMBER(20)	The unique number that EHRI will assign to an employee to identify employee records within EHRI.	This field is currently assigned and stored within EHRI and should be left blank by providers.
5	17	Employee ID	Agency Subelement Code	VARCHAR(4)	Agency and, where appropriate, the administrative sub-division (i.e. subelement) in which a person is employed.	See the Guide to Personnel Data Standards.
6	991	Completed Training Unit	Training Title	VARCHAR(100)	Official title or name of the course or program completed by the employee.	
7	723	Completed Training Unit	Training Type Code	VARCHAR(4)	Code for type of training which has been completed by the employee.	See Appendix A of the OPM Guide to Human Resources Reporting.

ICD Seq #	EHRI Ref #	Data Concept	Name	Datatype	Definition	Notes
8	1036	Completed Training Unit	Training Sub Type Code	VARCHAR(4)	Code for sub-type of training which has been completed by the employee.	See Appendix A of the OPM Guide to Human Resources Reporting.
9	720	Completed Training Unit	Training Start Date	DATE	Start date of the training completed by the employee.	
10	710	Completed Training Unit	Training End Date	DATE	End date of the training completed by the employee.	
11	89	Completed Training Unit	Continued Service Agreement Expiration Date	DATE	The date to which an employee is obligated to remain in service as a stipulation for taking the training.	
12	90	Completed Training Unit	Continued Service Agreement Required Indicator	VARCHAR(2)	Indication that an employee is obligated to remain in service as a stipulation for taking the training.	Y=Yes, N=No, NA=Non Applicable
13	699	Completed Training Unit	Training Accreditation Indicator	VARCHAR(2)	Indicates if the training course offers accreditation.	Y=Yes, N=No, NA=Non Applicable
14	704	Completed Training Unit	Training Credit	DECIMAL(9.2)	Amount of academic credit hours or continued education units earned by the employee for the completed training.	
15	705	Completed Training Unit	Training Credit Designation Type Code	VARCHAR(4)	Code for the type of academic credit hours or continued education units.	See Appendix A of the OPM Guide to Human Resources Reporting.

ICD Seq #	EHRI Ref #	Data Concept	Name	Datatype	Definition	Notes
16	987	Completed Training Unit	Training Credit Type Code	VARCHAR(4)	Code representing the type of credit hours the employee received for the completed training.	01=Semester Hours, 02=Quarter Hours, 03=Continuing Education Unit, 04=N/A
17	709	Completed Training Unit	Training Duty Hours	DECIMAL(9.2)	Number of employee duty hours the employee used to complete the training unit.	
18	714	Completed Training Unit	Training Non Duty Hours	DECIMAL(9.2)	Number of employee non-duty hours for the completed training course.	
19	707	Completed Training Unit	Training Delivery Type Code	VARCHAR(4)	Code for the type of training delivery for the training course completed by the employee.	See Appendix A of the OPM Guide to Human Resources Reporting.
20	716	Completed Training Unit	Training Purpose Type Code	VARCHAR(4)	Code representing the purpose of the training completed by the employee.	See Appendix A of the OPM Guide to Human Resources Reporting.
21	718	Completed Training Unit	Training Source Type Code	VARCHAR(4)	Source of the training which has been completed by the employee.	See Appendix A of the OPM Guide to Human Resources Reporting.
22	713	Training Materials Cost	Training Materials Cost	DECIMAL(9.2)	Cost to the government for the training materials used during the training unit completed by the employee.	

ICD Seq #	EHRI Ref #	Data Concept	Name	Datatype	Definition	Notes
23	715	Training Per Diem Cost	Training Per Diem Cost	DECIMAL(9.2)	Cost of the per diem (meal, lodging, misc. expenses) for the training completed by the employee that was paid for by the Federal Government.	
24	721	Training Travel Cost	Training Travel Cost	DECIMAL(9.2)	Cost of the travel, excluding per diem, for training completed by the employee that was paid for by the Federal Government.	
25	722	Training Tuition and Fees Cost	Training Tuition and Fees Cost	DECIMAL(9.2)	The cost of the training tuition and fee for training completed by the employee that was paid for by the Federal Government.	
26	1038	Training Nongovernment Contribution Cost	Training Nongovernment Contribution Cost	DECIMAL(9.2)	Cost contributed by the employee or other non-government organizations for the training completed by the employee.	
27		Training Travel Indicator	Training Travel Indicator	VARCHAR(2)	Indicates if the employee traveled to attend the training course.	Y=Yes, N=No, NA=Non Applicable