Privacy Impact Assessment
for the

Laboratory Management System (LMS)

DHS/S&T/PIA-035

December 10, 2018

Contact Point
David Bennett
LMS Information System Security Officer
National Biodefense Analysis and Countermeasures Center
DHS Science and Technology
(301) 619-5472

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The National Biodefense Analysis and Countermeasures Center (NBACC) is a federally funded research and development center (FFRDC) and laboratory within the U.S. Department of Homeland Security's (DHS) Science & Technology Directorate (S&T). NBACC develops and applies methods to identify the means, method, and forensic signatures associated with a biological agent, biocrime, or bioterror investigation. This work guides DHS investments in vaccines, drugs, detectors, and other countermeasures to protect against biological terrorism. NBACC uses the Laboratory Management System (LMS) to facilitate and maintain a state of mission-related laboratory compliance with International Organization for Standardization (ISO) Standard ISO 17025 (general requirements for the competence of testing and calibration laboratories) and its laboratory registration with the Centers for Disease Control (CDC) and the U.S. Department of Agriculture (USDA). LMS assists NBACC in meeting its compliance, verification, and registration obligations under ISO 17025; federal, state, and local regulations; and DHS policies; and in reducing the likelihood of records mismanagement in its mission- related laboratory operations. LMS collects personally identifiable information (PII) from or about DHS workforce members (both government and contractors) who work with NBACC. The PII collected, used, maintained, and transmitted by LMS is limited to information on the training, credentials, and qualifications of that NBACC workforce to perform its FFRDC and DHS laboratory mission.

Overview

LMS is a system owned and accredited by S&T. Through its core capabilities, LMS facilitates NBACC's recordkeeping and reduces the likelihood of record mismanagement. LMS and its core capabilities also enhances NBACC's ability to maintain its ISO General Requirements for the Competence of Testing and Calibration set forth in ISO 17025.[1] LMS facilitates NBACC's on-going capabilities to verify its compliance with ISO 17025; federal, state, and local regulations; and DHS policies. LMS consists solely of application servers built on several commercial off the shelf (COTS) sub-systems using SQL databases. LMS is a Major Application that resides on the Science & Technology (SciTech) General Support System (GSS) network.[2] To support NBACC, LMS deploys 11 NBACC core capabilities. Only one of these capabilities, Training, collects, uses, disseminates, or maintains PII.[3]

---

[1] ISO 17025 specifies the general requirements for the competence, impartiality, and consistent operation of laboratories and is applicable to all organizations performing laboratory activities, regardless of the number of personnel. Laboratory customers, regulatory authorities, organizations using peer assessment, and accreditation authorities use ISO 17025 in confirming or recognizing the competence of laboratories such as NBACC. For more information, please *see* https://www.iso.org/standard/66912.html.

[2] SciTech GSS allows secure communication and data exchange between S&T laboratories located around the United States, other S&T remote sites, and the DHS S&T headquarters in Washington, D.C. The SciTech Support Service provides IT security in the form of intrusion detection, prevention, encryption, and anti-virus/malware protection.

[3] Other deployed LMS core capabilities include Document Control/Management; Case R&D/Management; Communications Management; Corrective and Preventive Actions; Quality System Management; Internal Auditing;

DHS contractor workforce members supporting NBACC provide the following PII relating to their mission-related training and experience for input into the LMS database: first and last name; employee identification number; work address, work email address, work telephone number(s); employment history; education history; and job-related training and certifications (collectively, "training-related PII"). Contracting organizations provide training-related PII to the NBACC for individuals assigned to work there. To the extent training-related PII is necessary from DHS employees, the information is generally available from DHS-maintained employment records, such as those from the DHS Performance and Learning Management System (PALMS).[4] NBACC personnel manually enter all training-related PII it collects into LMS. LMS does not collect PII by a system-to-system interface or transfer and DHS forms are not used to collect contractor workforce training-related PII. Contractor workforce members' information is collected directly from the individual by the NBACC Training Coordinator, who is also a contractor, in the form of a certificate of training completion. The training-related PII in LMS is then applied to validate that the science conducted at the NBACC is accomplished by qualified trained personnel as required for laboratory facilities that meet ISO 17025 accreditation requirements.

Training-related PII in LMS may be shared with the CDC and other federal agencies including DHS, or third-party assessors in connection with their audits, assessments, and/or laboratory certifications of NBACC, and the Federal Bureau of Investigation (FBI) to facilitate forensic analysis and rules of evidence. Training-related PII is exported from LMS to share with external agencies because the PII is not shared directly through system-to-system transfers. This sharing is consistent with the purposes for which LMS collects training-related PII from its workforce members. All input to and output of training-related PII is done through DHS-owned workstations that are part of the SciTech GSS network.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

NBACC is an FFRDC sponsored by DHS S&T for the purpose of performing, analyzing, integrating, supporting, and managing basic or applied research and development. NBACC was DHS's first laboratory built for DHS as part of DHS's implementation of Presidential Directive HSPD-10 (2004).[5] Battelle National Biodefense Institute, LLC (BNBI) was selected by DHS in 2006 to manage and operate the facility as an FFRDC in 2006 and assumed operational control and management of the NBACC Laboratory facility in 2010. BNBI acts under the provisions of an

Administrative Functions; Lab Data and Sampling Analysis; Multi-Media Management; and Dynamic Reporting. These core capabilities do not collect, use, or disseminate PII.

[4] *See* DHS/ALL/049 Performance and Learning Management System (PALMS), *available at* https://www.dhs.gov/privacy.

[5] HSPD-10, Biodefense for the 21st Century, February 11, 2004, *available at* https://fas.org/irp/offdocs/nspd/hspd-10.html.

FFRDC Management and Operating Contract with DHS (M&O Contract) and the terms of that contract are governed by Federal Acquisition Regulation (FAR) Part 35 Federal Research and Development Contracting, Subpart 35.017 – Federally Funding Research and Development Centers.[6] Activation of NBACC's high containment laboratories was accomplished through registration with the CDC and USDA in 2011.The M&O Contract with DHS S&T is the primary agreement requiring the collection of mission-related PII information within LMS.

The M&O Contract and its CDC/USDA registration requires NBACC to collect and maintain the training and certification information of NBACC lab personnel. Additionally, the M&O Contract requires laboratory operations to be ISO 17025 accredited. It is also an ISO 17025 requirement to collect and maintain this information. Furthermore, to be a registered laboratory, NBACC must meet CDC select agent regulations,[7] and follow the *Biosafety Microbiolgical and Biomedical Laboratories* guidance for Biological Select Agents and Toxins (BSAT) handling,[8] which includes the requirement to staff the laboratories with fully qualified personnel and validate that staff is qualified. LMS satisfies all these requirements by collecting and maintaining the required information.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

LMS is covered by the following existing SORNs:

- OPM/GOVT-1 General Personnel Records,[9] which covers records reflecting work experience, education level achieved, and specialized education or training obtained outside of federal service;
- DHS/ALL-003 Department of Homeland Security General Training Records,[10] which covers records relating to training given to DHS employees, contractors, and others who are provided DHS training, and
- DHS/ALL-021 Department of Homeland Security Contractors and Consultants,[11] which covers records relating to contractor mission-related training, licenses, and certifications not covered under OPM/GOVT-1 and DHS/ALL-003.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

LMS was assessed through its Federal Information Processing Standard Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, documentation to be a Moderate Impact system. LMS currently has an Authority to Operate which

[6] http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/35.htm#P128_25711.
[7] 7 CFR part 331.15: Agriculture, 9 CFR part 121: Animals and Animal Products, 42 CFR part 73: Public Health
[8] CDC 5th Edition, *available at* https://www.cdc.gov/biosafety/publications/bmbl5/BMBL.pdf.
[9] OPM GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[10] DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).
[11] DHS/ALL-021 Department of Homeland Security Contractors and Consultants, 73 FR 63179 (October 23, 2008).

was granted on May 26, 2016. As part of the Authority to Operate process, LMS has a DHS S&T approved System Security Plan (SSP) and an approved System Privacy Plan (SPP).

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

At the present time, LMS does not have a records retention schedule approved by NARA. However, Records Schedule Number: DAA-0563-2017-0004; Request for Records Disposition Authority by DHS S&T Office of National Laboratories has been submitted to NARA and is pending. Under the pending records retention schedule, records that become part of a Law Enforcement Case file are retained for 20 years after the cut off (file is cut off at the submission of the final case report to the referring law enforcement agency), and then are to be destroyed, transferred to the appropriate law enforcement agency, or transferred to NARA to be kept permanently if significant and/or of public interest. If the record is not part of a Law Enforcement Case File, it is cut off at the end of the calendar year in which it was created and then is to be destroyed or retained as permanent (evaluated for significance and public interest) 20 years after the cutoff. The submitted records retention schedule will provide the retention period for all records maintained by the NBACC, to include all records maintained in LMS. Until the schedule is approved, LMS treats all its unscheduled records as permanent.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

LMS is not subject to PRA requirements because it does not collect information directly from the public. Contractor workforce training-related PII in LMS is entered manually from information provided by the contractor organization.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

LMS collects, uses, disseminates, or maintains PII that is limited to current and former NBACC workforce member training. That PII includes:

- First and last name;
- Employee identification number;
- Work address, work email address, work telephone number(s);
- Employment history;

- Education history; and
- Job-related training and certifications.

This training-related PII is necessary to validate that the research being conducted at the NBACC is being accomplished by qualified personnel. It is also necessary to meet ISO 17025 accreditation requirements. LMS does not create new PII. Training-related PII is manually maintained, after it is entered into LMS, by the NBACC Training Coordinator using Cybertrain, an application included in the LMS application suite. Cybertrain is certified and accredited by S&T.

2.2 What are the sources of the information and how is the information collected for the project?

PII is collected from contractor workforce members by the NBACC Training Coordinator for input into LMS. DHS employee training-related PII is collected from the DHS employee or DHS records and provided to the NBACC Training Coordinator for input into LMS. The contractor collects workforce training-related information solely to meet the requirements of its contract with S&T (which include being CDC registered for BSAT, ISO 17025 accredited, and meeting the memorandum of understanding (MOU) requirements between S&T and the FBI).

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

Collection of training-related PII on contractor workforce members supporting NBACC is the responsibility of the contractor, who also has responsibility for ensuring the accuracy of that information. In addition, contractor workforce members are responsible for providing the contractor accurate and up to date information on their education and work histories, employment history, job-related training, and certifications. These individuals may request the contractor to update and correct their records and to provide the updated/corrected information to the NBACC Training Coordinator for input into LMS. Similarly, DHS employees may update or correct their training-related PII by informing the NBACC Training Coordinator of changes or corrections to be made in LMS or by contacting S&T Human Resources.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that LMS is retaining more PII than necessary for documenting NBACC workforce members training, education, experience, and credentialing.

Mitigation: The NBACC Training Coordinator, who oversees the input of PII into LMS,

mitigates this risk by assuring that the only PII collected and input into LMS is that which is necessary to meet and document laboratory workforce member qualifications under applicable ISO, federal and state regulations, DHS policies, and other laboratory credentialing authorities. The Training Coordinator also ensures PII collected and maintained within LMS does not include sensitive PII (SPII), such as Social Security numbers or medical history.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

LMS uses the information to maintain a record of NBACC lab workforce member training. These training records are maintained within LMS and within the SciTech GSS network. LMS is not used to maintain SPII. PII in LMS is used to meet CDC and ISO 17025 accreditation requirements for the laboratory and NBACC's workforce, and to assure S&T that the laboratory workforce has and maintains the education, training, and professional credentials necessary to perform its individual and collective duties at the facility. In connection with forensic analysis performed by the laboratory under its MOU with the FBI, this information is used in court to prove NBACC meets evidentiary standards for performing forensic analysis that are used in criminal proceedings.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that unauthorized users may view the stored training-related PII or use that PII for unauthorized purposes.

Mitigation: This risk is mitigated. LMS uses role-based access controls to minimize what PII may be viewed or edited. Only specific authorized users have access to view or edit PII within LMS. All authorized users must authenticate to the SciTech GSS network using their Personal Identification Verification (PIV) credentials before accessing LMS applications. Users are only granted access to LMS applications based on their role and must then further authenticate to those applications containing PII using a unique username/password. All general users that have access to LMS have to successfully complete all S&T required IT and Security Awareness training and have read and acknowledged that they will abide by the SciTech/LMS Rules of Behavior. Additionally, privileged

users have to successfully complete additional training before they are granted access to LMS.

Privacy Risk: There is a risk that there may be an unauthorized disclosure of the PII maintained in LMS.

Mitigation: The risk is mitigated through NBACC physical and administrative controls. Access to PII in LMS is only permitted through DHS-owned workstations located on the SciTech GSS network and only LMS users authorized to access PII can do so. These users go through role-based and general privacy training. This risk is further mitigated because LMS is not a public facing system and has employed government security and privacy controls necessary for a system that contains PII. LMS application servers physically reside in a secure room with limited access, within a secure facility guarded by armed guards, and logically resides on the protected SciTech GSS network.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Contractors are contractually obligated to provide notice to their workforce prior to the collection of any training-related PII. Training-related PII is also collected directly from the contractor's workforce members by the NBACC Training Coordinator. The NBACC Training Coordinator gives verbal notice to the individual of the potential uses of their information at that time. The individuals voluntarily submit their training information, including certificates of training, either as hardcopy or as attachments to emails. Failure of an individual to submit his or her training information may result in the individual not being hired by the contractor or may limit the positions and responsibilities for which an individual is eligible. These records, when provided by the contractor to NBACC for including in LMS are records described in DHS/ALL-021 Department of Homeland Security Contractors and Consultants, and are voluntarily obtained from the contractor by whom the individual is employed.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

DHS contractors collect training-related PII directly from their workforce members for the purposes of working at NBACC. All individuals working at NBACC have a right to decline to provide training-related PII in connection with their work at NBACC at any time. If individuals decline to provide information, they may be ineligible to work at NBACC.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals providing training-related PII may be unaware that their information will be shared with the FBI, CDC, or other credentialing and accreditation organizations.

Mitigation: This risk is mitigated. Notice of the uses of that PII is provided verbally to individuals at the time their training-related PII is provided to the NBACC Training Coordinator for input into LMS. Individuals are informed in writing, with user acknowledgement, of the system Rules of Behavior and individuals are formally notified via the warning banner that is presented to the user each time they access LMS.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

The table below sets forth the applicable records retention schedules that have been requested through the Request for Records Disposition Authority pending with NARA.* Until the requested schedule is approved by NARA, LMS treats all its unscheduled records as permanent.

Records Schedule No*	Retention	Reason for Retention of Training Documentation
DAA-0563-2017-0004-0025	20 years	Used in Law Enforcement Cases for court
DAA-0563-2017-0004-0033	20 years	Research and Development Files or Projects, not used in Law Enforcement Cases
DAA-0563-2017-0004-0032	Permanent	Used in significant law enforcement cases or projects involving novel or complex issues, public interest, media attention or congressional scrutiny.
DAA-0563-2017-0004-0036	Destroy no sooner than 5 years after records have been superseded or become obsolete.	ISO 17025 Method Accreditation Records. Provide objective evidence of adherence to ISO standards at the time of sample analysis for law enforcement cases.

*DAA-0563-2017-0/004, 6/19/2018

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Records containing PII within LMS are currently not covered by a NARA-approved records retention schedule, which means that the records may be maintained longer than necessary for operations supported by LMS.

Mitigation: This risk remains unmitigated. Until LMS has a NARA-approved records retention schedule, NBACC is not legally permitted to dispose of these records. Pending approval of a NARA-approved records retention schedule, the records are considered permanent and not destroyed. However, records containing training-related PII are considered to be active records for

only six (6) years from the later of their creation or when the individual to whom those training-related records is no longer a member of the NBACC workforce. At that time, these records are removed from LMS by the Systems Administrators and prepared for archival/storage offsite. All archival tapes are encrypted and all paper copies are protected in accordance with S&T required security controls that have been implemented and verified via the Authority to Operate process.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

NBACC's M&O Contract with DHS S&T requires it to collect, maintain, and provide workforce member PII to the FBI, DHS, CDC, and other agencies as requested. The ISO accreditation process only verifies that NBACC has proper processes and training-related documentation on file, and training and experience PII is shown to ISO assessors, but not retained by them. DHS S&T has an MOU with the FBI on how information is requested, provided, and protected. The FBI commonly uses training-related PII in LMS to prove that forensic analyses conducted by NBACC meet the evidentiary standards of soundness in methodology and expertise when presented in criminal proceedings. To the extent that training-related PII in LMS is required in connection with NBACC's M&O Contract and its laboratory accreditation or credentialing by an authorized body, the authorized body must make a written request for that information to NBACC. The written request specifies the training-related PII sought and the individuals (or categories of individuals) in the NBACC workforce whose PII is to be provided. The NBACC Training Coordinator will then locate the requested training-related PII in LMS, output that PII, and provide the PII to the requestor. All responses to requests for information are provided electronically via the SciTech GSS email system.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

LMS's purpose is to facilitate and maintain a state of mission-related laboratory compliance with ISO 17025 and its laboratory registration with the CDC and the USDA. DHS shares information with the FBI, CDC, and others to demonstrate that compliance. The NBACC mission is to provide the scientific basis for the characterization of biological threats and bioforensic analysis to support attribution of their planned or actual use.

NBACC's work is regularly used as evidence in court proceedings. NBACC shares employee credentialing information with the FBI as part of the evidence package under Routine Use P of OPM GOVT-1, General Personnel Records, which allows disclosure of information to another federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a federal agency, when the Government is a party to the judicial or administrative proceeding. Sharing with the FBI is also covered by Routine Use A of DHS/ALL-003 Department of

Homeland Security General Training Records and DHS/ALL-021 Department of Homeland Security Contractors and Consultants of information to the Department of Justice (including United States Attorney's Offices) or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: . . . 4. The United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records."

NBACC must maintain its laboratory compliance with the CDC in order to meet its mission. NBACC shares employee credentialing information with the CDC pursuant to Routine Use D of DHS/ALL-003 Department of Homeland Security General Training Records and DHS/ALL-021 Department of Homeland Security Contractors and Consultants, which allows disclosure of information to an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

6.3 Does the project place limitations on re-dissemination?

DHS S&T is the system owner of LMS, as defined in the LMS SSP and Accreditation package. DHS contractually "owns" all information stored in LMS. DHS S&T has an MOU with the FBI on how information is requested, provided, and protected from dissemination of information. Anytime ISO audits an organization both parties agree upon a "Rules of Engagement," which state that any information gathered during the audit will be held in confidentiality and destroyed as soon as the audit report is completed.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

DHS S&T has an MOU with the FBI on how information is requested, provided, and protected. ISO audit agreements include what information will be requested by the auditors and how it will be protected. All responses to requests for information are provided via email. Emails are considered formal records and a copy of all emails are stored on SciTech GSS email servers.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Information may be disclosed to external entities, and possibly re-disseminated, for unauthorized purposes.

Mitigation: This risk is partially mitigated. Training-related PII in LMS is not released to a requestor unless the request is made to NBACC in writing. DHS S&T has an MOU with the FBI on how information is requested, provided, and protected. ISO audit agreements include what information will be requested by the auditors and how it will be protected by ISO. However, NBACC is not a party to an MOU with the CDC, and S&T does not place any restrictions upon the CDC

regarding training-related PII NBACC provides to the CDC in connection with maintaining NBACC's CDC/USDA laboratory registration. The CDC is responsible for safeguarding training-related PII provided to it in connection with laboratory registration, as well as its further use and disclosure of that training-related PII.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

All individuals (whether as current or former DHS employees or as members of a contractor's workforce) with PII in LMS can access their individual records by submitting a Privacy Act request for access to the individual's records in accordance with 6 CFR part 5. Forms for submitting a request may be obtained from the DHS Chief Privacy Officer and Chief Freedom of Information Act Officer, *https://www.dhs.gov/foia* or 1-866-431-0486. They may also contact the NBACC Training Coordinator to access their PII in LMS. Members of an NBACC contractor workforce with PII in LMS may also contact that contractor's human resources department for copies of their training-related PII the contractor provided to the NBACC Training Coordinator.

Individuals may also request access to information about them in LMS pursuant to the applicable provisions of the Freedom of Information Act (FOIA). An individual may submit a FOIA request to S&T by mail to: S&T FOIA Coordinator, Mail Stop: 0210, Department of Homeland Security, 245 Murray Lane, SW, Washington, D.C. 20528.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may submit requests to contest or amend information in LMS through the same procedures discussed in Section 7.1. Individuals who are U.S. citizens or lawful permanent residents may request corrections to or changes to their records through a Privacy Act request. All individuals may request corrections of erroneous PII through the NBACC Training Coordinator or the respective human resources department of their employer.

7.3 How does the project notify individuals about the procedures for correcting their information?

Information regarding how training information is entered into LMS and how individuals can access their training records is included in the NBACC Training and Development Standard Operating Procedure (010-005-SOP). All NBACC personnel are required to read and acknowledge that they understand the information in that SOP.

Public notice of the procedures for correcting information in LMS is provided to individuals through each of the SORNs referenced in Section 1.2, the Privacy Act Statements provided in connection with the collection of PII under each of those SORNs, and this PIA. In addition, the S&T

Office of Security explains the process for correcting information in S&T information systems to new hires and contractors during S&T on-boarding activities.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Information in LMS regarding individuals may be inaccurate or incorrect and the related individual may not be aware that it is.

Mitigation: This risk is mitigated because the underlying source of an individual's training-related PII in LMS is the individual, either through the individual's direct submission of training-related PII to DHS for inclusion in LMS or, in the case of a contractor workforce member, directly to the contractor for inclusion in LMS. In addition, PII input into LMS is centralized through the NBACC Training Coordinator, the responsibilities of whom include ensuring that NBACC workforce's training information in LMS is accurate, correct, and updated in a timely manner.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The Information System Security Officers and Network/System Administrators review system-generated audit logs at least weekly for inappropriate or unusual activity, and report adverse findings to the System Owner and S&T Chief Information Security Officer, in accordance with the LMS SSP and NBACC Incident Response Plan. Additionally, annual self-assessments, by NBACC Information System Security Officers, as well as S&T annual security assessment review of LMS are conducted as required to meet FISMA requirements. These reviews are all documented in the enterprise wide DHS Information Assurance Compliance System.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

DHS S&T mandated annual Privacy Training, Security Awareness Training, and Privileged User training (for individuals with privilege user accounts).

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

LMS uses role-based access controls. Personnel are granted the minimum level of access to information based on their organizational role. A formal, documented identification and authentication policy and procedure is included in the LMS SSP. The LMS SSP has been validated to meet all S&T access control requirements.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

DHS S&T owns all information maintained in LMS and has an MOU with the FBI on how information is requested, provided, and protected. Any "new" agreement would be negotiated and agreed to by DHS S&T. DHS S&T has a formal review and approval process in place for new sharing agreements. Any new use of information in LMS must be approved by the proper authorities at DHS, such as the DHS S&T Privacy Officer and the Office of General Counsel.

Responsible Officials

Lewis Brown
Program Manager, Labs Operations
Office of National Labs
Research and Development Partnerships
Science and Technology Directorate
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security