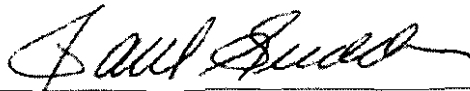


Privacy Impact Assessment

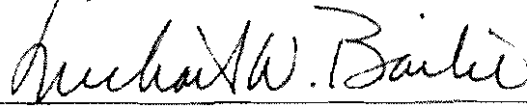
for the
JUSTLearn Learning Management System

Certifications:


I certify that this Privacy Impact Assessment conforms to the principles of OMB Memorandum M-03-22, and the assessed system is in compliance with Section 208 of the E-Government Act of 2002 (Pub. L. No. 107-347; 44 U.S.C. § 3501, *note*).

5/22/2007


Paul SuddesDate
Program Manager, JUSTLearn Learning Management System
Executive Officer, Office of Legal Education/National Advocacy Center
Executive Office for United States Attorneys
U.S. Department of Justice

5/22/07

Michael BailieDate
System Owner, JUSTLearn Learning Management System
Director, Office of Legal Education/National Advocacy Center
Executive Office for United States Attorneys
U.S. Department of Justice

5/23/07

William G. Stewart, IIDate
Assistant Director, Freedom of Information & Privacy Staff
Executive Office for United States Attorneys
U.S. Department of Justice

5/24/07

David W. DownsDate
Acting Chief Information Officer
Executive Office for United States Attorneys
U.S. Department of Justice

System Description: The JUSTLearn Learning Management System ("JUSTLearn") is a web-based computer system used to track training provided by the Office of Legal Education/National Advocacy Center (OLE/NAC). The mission of the NAC is to provide legal education and training to federal, state, and local prosecutors, litigators, and support staff, with an average of 14,000 individuals receiving training annually. The NAC is operated by OLE and is located at 1620 Pendleton Street Columbia, SC 29201, on the campus of the University of South Carolina. Additional information about OLE/NAC can be found on the DOJ web site (<http://www.usdoj.gov/usao/eousa/ole>).

The JUSTLearn system is operational, but it is accessible only to authorized users.

System Purpose: JUSTLearn allows OLE/NAC to track training courses and report to the Office of Personnel Management (OPM) in accordance with 5 C.F.R. 410.701, which states in pertinent part as follows:

(a) Each agency shall maintain records of training plans, expenditures, and activities in such form and manner as necessary to submit the recorded data to the Office of Personnel Management (OPM) through the OPM Governmentwide Electronic Data Collection System.

(h) Beginning December 31, 2006, each agency shall report the training data for its employees' training and development at such times and in such form as required for the OPM Governmentwide Electronic Data Collection System, which is explained in the Guide to Personnel Recordkeeping and the Guide to Human Resources Reporting.

See 5 C.F.R. 410.701 (available via GPO-Access/eCFR at: <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=c9288c047019e90e5ebf91151b1b23c&rgn=div8&view=text&node=5:1.0.1.2.57.7.16.1&idno=5>).

Assessment:

1. What information is to be collected?

The type/quantity of data collected are trainee contact info (e.g., address, phone, email, supervisor) and personal identifiers (e.g., name, title, SSN (last 4 digits)).

2. Why is the information being collected?

The information is collected in order to track OLE/NAC training courses and report to OPM pursuant to 5 C.F.R. 410.701.

3. What is the intended use of the information?

The intended use of the information is to facilitate the presentation and evaluation of OLE/NAC training courses and report to OPM pursuant to 5 C.F.R. 410.701.

4. With whom will the information be shared?

The information will only be shared with authorized users who have a legitimate need to know and with OPM, *e.g.*, pursuant to 5 C.F.R. 410.701.

5. What opportunity will individuals have to decline to provide information or to consent to particular uses of the information, and how individuals can grant consent?

As this information is required for the provision of OLE/NAC training and for OPM reporting purposes, individuals have no opportunity to decline to provide or consent to particular uses of the information.

6. How is the information being secured?

The information is secured with management, operational and technical controls as delineated by NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. The applied system category control set is **moderate** as defined by NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*. This system is certified and accredited for control compliance as well as adherence to industry security best practices and mitigation-of-risk due to technical vulnerabilities.

The potential risk for unauthorized disclosure for personal information 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; and
- monitoring network activity with a continuously monitoring intrusion detection system.

7. Is the system of records being created under the Privacy Act, 5 U.S.C. § 552a?

The information collected and maintained is covered by published systems-of-records under the Privacy Act as follows: OPM/GOVT-1, "General Personnel Records," 71 Fed. Reg. 35342 (June 19, 2006). The information may be disclosed without the individual's consent, but only as permitted by the Privacy Act, the Freedom of Information Act, and related agency regulations and procedures.