

DL Design Best Practices for PII

“Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as personally identifiable information (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual.” (DoD 5400.11, DOD Privacy Program, 8 May 2007, paragraph E2.2 and DoD 5400.11-R, Department of Defense Privacy Program, 14 May 2007, paragraph DL1.14)

Distributed Learning (DL) training and education products are produced for web-based delivery from the .mil domain. Although protected from viewing by the general public, the content is not protected from abuse by individuals who would seek to invade an individual's privacy or steal an individual's identity. There is no guarantee other than to follow the established guidelines for the protection of personally identifiable information (PII).

POTENTIAL PII

The use of social security numbers and other personally identifiable information (PII) is forbidden in web based courseware. With the rise of personal identity theft, we must be especially sensitive to the use of any information in the text or graphics that could jeopardize personal information. So how do we construct meaningful learning events for our students without compromising security of personal information?

- Depictions of social security numbers should follow the guidance of the Social Security Administration which recommends 111-22-3333 or similar scheme which does not present the possibility of a combination of a real number and corresponding name being used in the course. Even the possibility of this combination could delay or prevent fielding of the content.
- Name and rank of real soldiers depicted in web based training and education should follow all privacy guidelines under the Freedom of Information Act (FOIA). As a safeguard when using real soldiers, ensure they have completed DD Form 2833 (Oct 2000). This documentation should be sent to the TADLP COR and included in the contract file.
- Training on Army systems that require the learner to enter personal information such as SSNs, date of birth, name, and rank must be clearly fictitious.
- Screen captures of system databases such as a human resource or financial system; hold the greatest potential for PII breach. This must be a simulated capture of the database items

USING THE CAPDL CONTRACT

All Requesting Activities (RAs) that seek to use the Combined Arms Products for Distributed Learning (CAPDL) contract vehicle will ensure compliance with DoD and Army regulations and guidance and complete a MEMORANDUM OF UNDERSTANDING with the Office of the TCM TADLP.

DEFINITIONS

PII Breach

1. Definition of PII breach. A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. This includes, but it not limited to, posting PII on public-facing websites; sending via e-mail to unauthorized recipients; providing hard copies to individuals without a need to know; loss of electronic devices or media storing PII (for example, laptops, thumb drives, compact discs, etc.); use by employees for unofficial business; and all other unauthorized access to PII.

Additional information can be found at: http://www.tradoc.army.mil/Reporting_PII.asp

Freedom of Information Act (FOIA)

The Army Freedom of Information Act Office <https://www.rmda.army.mil/foia/RMDA-FOIA-Division.html> is responsible for management oversight of the Army-wide implementation of the Freedom of Information Act (FOIA) program in accordance with 5 USC, and Public Law 106-554. The office implements the Office of Management and Budget (OMB), Department of Justice (DOJ) and Department of Defense (DoD) guidance regarding the FOIA and ensure the requirements of Executive Order (EO) 13392 (Improving Agency Disclosure of Information) and the Action Plan are fulfilled. This office is not a repository of documents but can forward requests for specific information to the appropriate authority.

Additional information can be found at: <http://www.tradoc.army.mil/FOIA.asp>