August 26, 2014

DIRECTIVE:	JOB CORPS PROGRAM INSTRUCTION NOTICE No. 14-09

TO: ALL JOB CORPS NATIONAL OFFICE STAFF
ALL JOB CORPS REGIONAL DIRECTORS
ALL JOB CORPS CENTER DIRECTORS
ALL JOB CORPS CENTER OPERATORS
ALL NATIONAL TRAINING AND SUPPORT CONTRACTORS
ALL OUTREACH, ADMISSIONS, AND CTS CONTRACTORS

FROM: LENITA JACOBS-SIMMONS
Acting National Director
Office of Job Corps

SUBJECT: Reminder to Protect Job Corps Students' Personally Identifiable Information (PII)

1. Purpose. To remind the Job Corps community of the importance of protecting students' information.

2. Background. A mobile application for iPhone and Android was available to the public. This application exposed student names and class schedules for a particular Job Corps center. Sharing this type of personal information with the public could result in harm to the students (for example, a stalker finding out exactly where a student is at a certain time of day). This particular application has been taken down. However, this occurrence serves as a reminder of the critical responsibility that every staff member in Job Corps has to protect students' personal information.

3. Action. PII may include any information that *distinguishes* an individual (e.g., first/last name, social security number, date of birth, photo/biometric, etc.), and any information that may be *linked* to an individual (e.g., educational, medical, financial, address/phone number, background records, etc.).

PII must be treated as sensitive information and, as such, requires special handling and consideration at all times. It does not matter what medium is being used (e.g., iPhone application or other custom application, custom spreadsheet, printed reports, e-mails, packages, folders, or any other medium) - PII must be protected.

- Sharing – Job Corps student PII should only be shared on a need-to-know basis: always take a moment to consider whether it is absolutely necessary to share the

information; and whether the person receiving it has a need to know, and is authorized to view it.

- Transporting – When sending PII electronically, it must be encrypted during transmission (e.g., e-mail on your Citrix desktop, not through your personal e-mail); when sending a hard copy in the mail, it must be double-sealed.

- Storing – All PII stored on a hard drive, flash drive, or disk must be encrypted. All PII in physical form must be protected as well (e.g., in a locked drawer or filing cabinet, not left lying unattended on a desk).

- Disposing – PII must be disposed of in such a manner that the information cannot be recovered (e.g., shredded).

A suspected loss or compromise of PII must be reported **within 1 hour** to the Job Corps Technical Assistance Center (TAC) at (800) 598-5008, Option 4. If the incident occurs after working hours (7 p.m. – 7 a.m. Central), contact TAC and select Option 7 to report a PII incident.

4. Expiration. Until superseded.

5. Inquiries. Inquiries should be directed to Christopher Cale (888) 886-1303 x7223, cale.chris@jobcorps.org; or Linda Estep (888) 886-1303 x7212, estep.linda@dol.gov.