September 22, 2006

DIRECTIVE: JOB CORPS PROGRAM INSTRUCTION NO. 06-08

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: ESTHER R. JOHNSON, Ed. D.
                    National Director
                    Office of Job Corps

SUBJECT: Use of Computer Applications Containing Job Corps Students Personally
                    Identifiable Information

1.   Purpose. To provide guidelines for the use of computer applications containing Job
Corps Students' Personally Identifiable Information (PII).

2.   Background. Safeguarding sensitive information and protecting the Job Corps student's
privacy is a critical responsibility that must be taken seriously at all times. On June 29, 2006, the
National Office of Job Corps issued Program Instruction 05-26 to conduct a survey to identify all
computer systems that may contain PII of Job Corps students. The survey results revealed that
many centers, Outreach and Admissions (OA)/Career Transition Service (CTS) agencies,
National Training Contractors (NTCs), and support agencies maintain local databases that
contain PII data, without necessary security controls and assessments. Many of these systems
are in the form of home-grown MS Access databases or similar databases that lack security
features and are not part of the approved DOL Enterprise Architecture (EA). These systems are
considered high risk, and immediate action must be taken to eliminate these systems and protect
Job Corps students' personal data.

        Any personal data of Job Corps students, from which the student's identity is apparent, or
can reasonably be ascertained, is considered PII data. These include but are not limited to the
following:
        •   Name
        •   Date of Birth
        •   Social Security Number

- Other number originated by a government that specifically identifies an individual
- Photographic Identifiers (e.g., photograph image, x-rays, and video)
- Driver's License
- Biometric Identifiers (e.g., fingerprint and voiceprint)
- Mother's Maiden Name
- Vehicle Identifiers (e.g., license plates)
- Mailing Address
- Phone Numbers (e.g., phone, fax, and cell)
- Medical Records Numbers
- Medical Notes
- Financial Account Information and/or Numbers
- Certificates (e.g., birth, death, and marriage)
- Legal Documents or Notes (e.g., divorce decree, criminal records, etc.)
- Device Identifiers (e.g., pacemaker, hearing aid, etc)
- Web URLs
- Email Address
- Education Records

3.   Action. The Career Development Service System (CDSS) Suite of Applications developed and maintained by the National Office is the primary computer system to be used by the Job Corps community to manage Job Corps student information. Use of any other computer applications containing Job Corps students PII data must be approved by the National Director or designee.

In cases where third party applications are required for Job Corps student training and service (such as Charter Schools, local school district systems, etc), Job Corps center and agency staff must request that third party partners eliminate the use of Job Corps students' Social Security Numbers and Dates of Birth, and ensure they have all necessary security controls in place to protect Job Corps students' personal data.

National Office Division Chiefs and Regional Directors and will receive detailed reports of the survey results for contracts within their region and division, with recommendations from the National Office Technical Team. National Office Division Chiefs and Regional Directors must ensure corrective action is taken immediately.

4.   Expiration. Until superseded.

5.   Inquiries. Inquiries should be directed to Linda Estep at estep.linda@dol.gov.