March 19, 2007

DIRECTIVE: JOB CORPS PROGRAM INSTRUCTION NO. 06-23

TO: ALL JOB CORPS NATIONAL OFFICE STAFF
              ALL JOB CORPS REGIONAL OFFICE STAFF
              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: Guidance on the Safekeeping of Forms, Records, and Other Hardcopy
              Documents Containing Personally Identifiable Information

1.   Purpose. To provide guidelines for the safekeeping and accountability procedures
necessary to protect Personally Identifiable Information (PII) contained in forms, records, and
other hardcopy documents.

2.   Background. Safeguarding sensitive information and protecting the Job Corps student's
and employee's privacy is a critical responsibility that must be taken seriously at all times. In
light of previous breaches of information containing PII at other government agencies, on
July 12, 2006, the Office of Management and Budget (OMB) issued Memorandum M-06-19
requiring that all incidents involving PII be reported **within 1 hour** of discovering the incident.
The Federal Information Security Management Act of 2002 requires all agencies to report
security incidents to a federal incident response center.

      The National Office of Job Corps initially focused its efforts on the problem from the
technological perspective and issued Program Instruction No. 05-26 to survey the Job Corps
community concerning computer systems with PII. Program Instruction No. 06-08 then
provided guidance on protecting PII. The Job Corps Data Center (JCDC) also issued JCDC
Notice 05-275 to further convey guidance to the Job Corps community. Most recently, Program
Instruction 06-13 provided guidance on the reporting of incidents involving loss, unauthorized
disclosure, or unauthorized distribution of Job Corps students' PII information and informed the
Job Corps community of the requirements of the Department of Labor (DOL) and OMB.

3.   Definition.   Program Instruction No. 06-08 defined PII as follows: "Any personal data of Job Corps students, from which the student's identity is apparent, or can reasonably be ascertained, is considered PII data." PI data are not limited to the items that follow but often times will appear in combination on the forms:

- Name
- Date of Birth
- Social Security Number
- Other numbers originated by a government that specifically identify an individual
- Photographic Identifiers (e.g., photograph image, X ray, 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
- E-mail Address
- Education Records

4.   Action. The following responsibilities and procedures shall be in place by July 1, 2007:

   a.   **Center Directors:**

   (1)   Designate a secure central area for the maintenance of all student and employee files and records.

   (2)   All student/employee files must be secured in a locked filing cabinet or similar secure storage container.

   (3)   Health and counseling records must be secured in a locked filing cabinet or similar storage container in the respective areas.

   (4)   A designated staff must be appointed to access the secured files, and provide the name(s) of the designated staff to the Regional Office
   .

   (i)   Human Resources for employee files.
   (ii)   General Administration for student files.

(5)   An up to date inventory of all files must be established and maintained as well as maintenance of a sign-out log to ensure that all files containing PII are accounted for at all times.

b.   **National and Regional Offices, Center Operators, National Training and Support Contractors and OA/CTS:**

(1)   A secure central area for the maintenance of all Job Corps related documents must be designated.

(2)   A designated staff with access to secured files must be appointed.

The National and Regional Offices, Center Directors, national training and support contractors, and OA/CTS contractors must follow the same guidelines for the reporting of incidents involving loss, unauthorized disclosure, or unauthorized distribution of Job Corps students' PII as outlined in OMB Memorandum M-06-19 and Program Instruction 06-13. The incident response center for the Job Corps community is accessed by contacting the Job Corps Technical Assistance Center (TAC) at (800) 598-5008.

All forms or other hardcopy documents containing student or employee PII are to be kept in either the student or employee file. The Attachment is a list of Job Corps forms containing PII.

Addressees are to ensure that a copy of this Program Instruction is distributed to all appropriate staff immediately.

5.   Expiration Date. Until superseded.

6.   Inquiries. Inquiries should be directed to Linda Marshall at (202) 693-3106 or marshall.linda@dol.gov.

Attachment

Job Corps Forms Containing Personally Identifiable Information