April 12, 2007

DIRECTIVE:	JOB CORPS PROGRAM INSTRUCTION NO. 06-25

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: Enforcement of Personally Identifiable Information Policy and Procedures

1. Purpose. To enforce Job Corps previous requirements for protecting Personally Identifiable Information (PII) and to ensure removal of all applications and systems that contain Protected PII. For the purposes of this Program Instruction, systems that reside outside of the Career Development Services System (CDSS) suite of applications are considered third-party applications. Such applications are now prohibited from collecting, storing, transmitting, retrieving or containing any Job Corps PII. This definition encompasses all autonomous applications, independent databases, portable storage devices, spreadsheets, tables, documents, removable media, images or pictorial representations of protected PII that may exist outside the security perimeter of the Job Corps network. The CDSS suite of applications is the only sanctioned venue within which Job Corps protected PII may reside.

Included with this Program Instruction is further information from the Department of Labor (DOL) regarding protected PII and program guidance from Job Corps on implementing protection measures for PII. This Program Instruction also serves to notify the Job Corps community of upcoming PII audits that will be conducted by the Job Corps Security Team.

2. Background. In the wake of recent incidents involving the loss of PII, new requirements have been issued and mandates strengthened to assure that sensitive information is protected at all times. Job Corps has already taken the following actions to protect PII:

a. Released Job Corps Data Center Notice 05-275 dated May 26, 2006, DOL Policy on Safeguarding Personally Identifiable Information.

b. Released Job Corps Program Instruction No. 05-26 dated June 29, 2006, Survey of Computer Systems Containing Personally Identifiable Information of Job Corps Students.

c. Released Job Corps Program Instruction No. 06-08 dated September 26, 2006, Use of Computer Applications Containing Job Corps Students Personally Identifiable Information.

d. Released Job Corps Program Instruction No. 06-13 dated November 3, 2006, Reporting Incidents Involving Job Corps Students' Personally Identifiable Information.

e. Released Job Corps Data Center Notice 06-098 Certification of Removal of PII with attached draft of PII and Job Corps PII Policy December 13, 2006

f. Effective October 20, 2006, all Web site access to CDSS applications was disabled as a result of recent mandates. Job Corps users who require access to the CDSS applications must now use the Job Corps Citrix portal.

Additionally, Job Corps Program Instruction No. 06-08, Use of Computer Applications Containing Job Corps Students Personally Identifiable Information, dated September 22, 2006, notified the Job Corps community that:

a. The CDSS suite of applications is the only authorized system for capturing and maintaining student personal information.

b. All third-party systems that contain student protected PII must be eliminated. These third-party systems are considered high risk because they lack required security features and are not part of the approved DOL Enterprise Architecture.

A survey (published in Program Instruction No. 05-26, Survey of Computer Systems Containing Personally Identifiable Information of Job Corps Students, dated June 29, 2006) of computer systems used at centers revealed that more than 140 such applications are currently in use. These systems must be eliminated. The attached certification form (Attachment A) is to be used to verify that these systems have been turned off and the data in those systems destroyed. The form must be completed and signed by the system's principal owner or an authorized designee of that owner with signature authority for their organization. Signatories as the principal system owner may include Center Directors, Outreach and Admissions/Career Training Service (OA/CTS) Managers, Program or Project Managers, corporate officers or other organization official authorized to sign on behalf of their organization. This "principal system owner" must clearly identify themselves by providing their full name, the name of their organization, their company title, and their contact information on the returned certification form.

3. Action. Effective immediately, all Job Corps principal system owners of any application containing protected PII must complete Attachment A, including all required contact information. The principal system owner must then fax the signed and completed form to Job Corps Data Center (JCDC) Security at (512) 804-2002. **Forms must be returned by May 11, 2007.** If you have already sent in your certificate, you do not need to resend it.

All protected PII data previously gathered through use of these applications or generated reports must be destroyed as defined in the attached policy (Job Corps: Protecting Personally Identifiable Information (PII) Policies and Procedures—Attachment B). The Job Corps Security Team has been empowered to begin conducting PII security audits any time after the May 11th deadline to ensure compliance.

NOTE: Please submit a request for enhancement to the CDSS suite of applications if you currently use an application (other than CDSS) that gathers or stores protected PII and wish to retain this functionality. Examples include: Identification and Badging systems or applications used to store medical information. These requests will be prioritized by Job Corps management and implemented as quickly as resources and budgets allow. Priority ranking will be based on requests that provide the highest value to the greatest number of users in the Job Corps community.

4. Expiration. Until superseded.

5. Inquiries. Inquiries should be directed to Lori McElroy at mcelroy.lori@jobcorps.org or Linda Estep at estep.linda@dol.gov.

Attachments

A – Certification for Removal of Third-Party Applications Containing Personally Identifiable Information

B – Job Corps: Protecting Personally Identifiable Information (PII) Policies and Procedures