November 3, 2006

┌───┐
DIRECTIVE: JOB CORPS PROGRAM INSTRUCTION NO. 06-13
└───┘

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: Reporting Incidents Involving Job Corps Students' Personally Identifiable
                 Information

1.   Purpose. To provide guidelines for the reporting of incidents involving loss, unauthorized disclosure, or unauthorized distribution of Job Corps students' Personally Identifiable Information (PII) and to inform the Job Corps community of the requirements of the Department of Labor (DOL) and Office of Management and Budget (OMB).

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. The National Office of Job Corps issued Program Instruction No. 05-26 to survey the Job Corps community concerning computer systems with PII. In additional, Program Instruction No. 06-08 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.

        On July 12, 2006, OMB issued Memorandum M-06-19 requiring 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 incident response center for the Job Corps community is accessed by contacting the Job Corps Technical Assistance Center (TAC) at 800-598-5008.

        Action. All Job Corps staff must be notified immediately that any incident involving PII must be reported to supervisors and management within 1 hour of discovering the incident. All incidents involving PII, in either electronic or physical form, must be reported. All Job Corps staff need to understand what constitutes PII and the importance of protecting it at all times.

If an actual or suspected incident occurs that involves the loss or unauthorized disclosure or distribution of PII in electronic or physical form, it must be reported **within 1 hour** to Job Corps TAC at 800-598-5008. If the incident occurs after working hours (between 7pm-7am CST), contact TAC and follow the prompts to report a PII incident. A member of the Job Corps Computer Security Incident Response Team (CSIRT) will respond and request that you email the attached form with the PII incident details to jcdcsecurity@jobcorps.org. **DO NOT** send the incident form without speaking to a CSIRT team member as this is a time-sensitive incident that must be escalated to the National Office of Job Corps within 1 hour of reporting.

It is the responsibility of every Job Corps employee to ensure that PII is protected at all times, and to immediately report any circumstance or incident which may indicate the loss or compromise of such information.

4.   Expiration. Until superseded.

5.   Inquiries. Inquiries should be directed to Lori McElroy at 888-886-1303 x7404 or mcelroy.lori@jobcorps.org, or Linda Estep at 888-886-1303 x7212 or estep.linda@dol.gov.

Attachment

Job Corps Personally Identifiable Information (PII) Incident Reporting