July 18, 2006

DIRECTIVE: JOB CORPS PROGRAM INSTRUCTION NO. 06-02

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
National Director
Office of Job Corps

SUBJECT: Mandatory Annual Account Re-certification for Center Information System, Career Transition System, Outreach and Admission Student Input System Applications Using the Job Corps Segregation of Duties and Account Management Policies and Procedures

1. Purpose. To notify the Job Corps community of the federal requirements, policies and guidelines associated with Center Information System (CIS), Outreach and Admission Student Input System (OASIS), and Outreach and Admission Student Input System (CTS) Account Re-Certification process. To provide updated copies of these policies and outline the 2006 Account Re-Certification process. The Segregation of Duties and Account Management Policies should be used to ensure procedures are in place to limit staff access to only those functions necessary for their job and enforce general account maintenance procedures. These policies, procedures and guidelines are necessary to maintain data integrity and must be followed by the Job Corps community at all times.

2. Background. Job Corps continues to ensure compliance with federal security requirements, the Job Corps Segregation of Duties, Account Management Policies and Procedures by conducting an annual Account Re-Certification audit for CIS, OASIS, and CTS.

3. Action. Regional Offices and Job Corps center operators must ensure compliance with the following. Effective immediately, Job Corps Center Directors, Outreach and Admissions (OA)/CTS contract managers and Points of Contact (POC) must:

a. Policy review:

(1) Read the Segregation of Duties and Account Management documents (Attachments A and B).

(2) Ensure these policies and procedures are incorporated into the agency's Standard Operating Procedures (SOP). If any exceptions exist as defined below in Section 4, Exceptions, it will be necessary to request approval from Job Corps Data Center (JCDC) Security to use compensating controls and provide supporting documentation by August 21, 2006.

(3) If any of these exceptions exist, please contact jcdcsecurity@jobcorps.org for further instructions.

b. For CIS Re-Certifications:

(1) Review the CIS Account Re-Certification Instructions (Attachment C).

(2) Verify and update all user accounts and user account profiles using the instructions.

c. For CTS and OASIS Re-Certifications:

(1) Review the CTS Account Re-Certification Instructions (Attachment D) and the OASIS Account Re-Certification Instructions (Attachment E).

(2) Review the list of user accounts and profiles provided by the JCDC to each Center Director, POC, and OA/CTS Contract Manager**. Lists for CTS and OASIS will be sent in a separate communication from the JCDC.**

(3) Verify and update all user accounts and user account profiles using the instructions.

d. Send the following to the attention of the JCDC Security team via fax at **512-804-2002 by COB August 21, 2006.**

The attached Account Re-Certification form (Attachment G) for CIS, OASIS, and CTS, certifying accounts have been verified and updated in compliance with the Segregation of Duties and Account Management

Policies. **If appropriate, there could be three separate forms that should be returned, one for CIS, OASIS, and CTS. These forms must be signed and dated by the application POC and the Center Director or contracting official**.

e. Participate in spotlight training on the process for re-certification of accounts and address questions during the training session. This training will be available in SIMON beginning July 25, 2006. Additional Q&A sessions will be scheduled in the weekly POC and Polycom conference calls.

4. Exceptions to the Segregation of Duties. In those instances where duties and system access to critical system functions cannot be fully segregated (normally due to staffing constraints), compensating controls must be established (at each location) as appropriate. Compensating controls are additional procedures designed to reduce the risk of errors, irregularities or fraudulent activities.

Procedures could include such controls as maintaining logs, monitoring staff activities, dual authorization requirements, and documented reviews of input/output. Special permission must be obtained by National or Regional Offices in addition to JCDC Security to qualify for use of a compensating control. These requests should be rare and must be accompanied by complete documentation including a justification and each compensating control to be used.

All records must be strictly maintained and periodic audits will be performed for those centers with compensating controls in place. If a condition exists that warrants an exception, first obtain National or Regional Office approval and forward this to jcdcsecurity@jobcorps.org for final approval and for archiving supporting documentation for audit purposes. (See Section 5 below, "Multiple System Access," as an example of a situation requiring a compensating control).

5. Multiple System Access. According to the Segregation of Duties Policies and Procedures, "No individual user should have access to all three student tracking applications - CIS, OASIS, and CTS - unless special authorization is obtained from the National or Regional Office. For example, the National Office authorizes an employee to have access to all three systems in order to conduct internal audits at Job Corps centers." If this condition exists for any user, it is necessary to complete the Authorization to Access Multiple Applications (Attachment F), obtain the required approvals, and submit these forms to JCDC Security, as well as maintain a copy onsite for future audits.

NOTE: According to the Account Management Policies and Procedures, all POCs must verify the approvals and requested accesses indicated on the New User ID Request form and keep a copy of this form on file for 1 year beyond the separation date

of the user. User ID request forms are available at the following Web site: **http://forms.jobcorps.org/datacenter/logins.htm**

6. Expiration Date. Until superseded.

7. Inquiries. Questions or comments may be addressed to Lori McElroy, (888) 886-1303 ext 7404 or mcelroy.lori@jobcorps.org, or Linda Estep, (888) 886-1303 ext 7212 or estep.linda@jobcorps.org, or the JCDC Technical Assistance Center at (800) 598-5008.

Attachment A – Job Corps Segregation of Duties Policies and Procedures
Attachment B – Job Corps Account Management Policies and Procedures
Attachment C – CIS Account Re-Certification Instructions
Attachment D – CTS Account Re-Certification Instructions
Attachment E – OASIS Account Re-Certification Instructions
Attachment F – Job Corps Authorization for Access to Multiple Applications
Attachment G – Job Corps Account Re-Certification Forms