June 23, 2003

DIRECTIVE:	JOB CORPS PROGRAM INSTRUCTION NO. 02-22

TO: ALL JOB CORPS NATIONAL OFFICE SENIOR 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: RICHARD C. TRIGG
National Director
Office of Job Corps

SUBJECT: Authorized and Secured Data Circuits at Job Corps Centers

1. Purpose. To inform the Job Corps Community of the requirement to ensure that data circuits at Job Corps centers are authorized and approved by the national office.

2. Background. Program Instructions 96-33 and 97-17 (Attachments A and B, respectively) outlined the Job Corps National Office policy for obtaining approval for data circuits at Job Corps centers.

An unauthorized third-party data circuit is defined as an electronic circuit installed between a Job Corps center and a third-party entity for the purpose of transporting data, without prior approval from the national office. Unauthorized data circuit types include:

- Digital Subscriber Lines (DSL)
- cable modems
- fractional T1s
- private lines
- connections to any Internet Service Provider (ISP), including modem dial-up, etc.

Unauthorized data circuits also include wireless access points or those connections to a third-party entity made without prior approval from the national office, since these connections may present a significant security risk to the Job Corps center network and to the Job Corps Community. Data circuits installed without engineered security precautions are portals for malicious attacks from the public Internet.

The consequences of unauthorized center network penetration will have an impact on the day-to-day operations on the Job Corps Community. The security risks associated with the use of unauthorized data circuits include the potential corruption of sensitive student information and/or causing production systems to become inoperable or unreachable.

3. Requirements. The Office of Inspector General (OIG) will continue to audit the Job Corps network to determine if the network is secure from penetration by malicious parties, and to ensure that federal security policies are being enforced. If the center network is successfully penetrated, actions will be taken to disconnect the Job Corps network from the public Internet. Therefore, it is critical that centers, center operators, and support contractors follow the procedures for obtaining national office approval prior to the installation of data circuits.

4. Action.

a. The national office will begin random security audits at Job Corps centers to determine if there are any unauthorized data circuits installed. Audits will be conducted onsite and remotely. If it is determined that there is an unauthorized circuit installed at a Job Corps center, the network connection to that center will be shut down until the unapproved data circuit has been removed or redesigned, so that it does not present a threat to the security of the Job Corps network. This also includes scanning utilities, routers and switches not approved by the national office that may compromise the Job Corps network security.

b. Job Corps centers that have data circuits installed without written consent from the national office must disconnect these circuits immediately. Any costs associated with rectifying the violation will be charged to the contractor responsible for that center.

c. All data circuits installed at a Job Corps center must be approved in writing by the national office. Centers not in compliance with this policy must contact Linda Estep of the national office via email at EstepL@jcdc.jobcorps.org no later than July 15, 2003, to obtain approval for the continued use of existing data circuits and proprietary systems.

d. New requests for additional connectivity should be sent in writing from the center director in conjunction with the center operator and/or support contractor to the: Job Corps Data Center, ATTN: Linda Estep, 205 Sixth Street, San Marcos, TX, 78666. Requests should include:

- justification for the connectivity;

- the applications and/or services that will be supported via this connectivity;

- point-of-contact information for the third-party entity; and,

- point-of-contact information for the Job Corps center.

e. The national office will coordinate a schedule for evaluating the requested infrastructure modification and will provide technical assistance, where needed, to comply with Job Corps security policies.

f. Addressees are to ensure that a copy of this Instruction is provided to appropriate staff.

5. Expiration Date. Until superseded.

6. Inquiries. Inquiries regarding this Instruction should be addressed to Linda Estep (EstepL@jcdc.jobcorps.org) of the national office, or Eric Vazquez (Vazqueem@jcdc.jobcorps.org) at the JCDC (800-598-5008).

Attachments:

A – Program Instruction 96-33, *Center Wiring/Office Automation Issues*

B – Program Instruction 97-17, *The Co-existence of Proprietary Center Information Systems and the Center Information System (CIS) Network Infrastructure and Schedule for Proprietary Systems Phase Out*