May 24, 2005

DIRECTIVE: JOB CORPS PROGRAM INSTRUCTION NO. 04-24

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 AND ADMISSIONS AND CTS CONTRACTORS

FROM: GRACE A. KILBANE
National Director
Office of Job Corps

SUBJECT: Job Corps Network Information Technology and Security Policies and Procedures

1. Purpose. (1) To define how access controls to protect the Job Corps network against unauthorized access are to be implemented throughout the Job Corps community; (2) establish and reiterate Job Corps Information Technology (IT) policies regarding Windows 95/98/2000/XP, hubs and unauthorized wireless devices, third-party circuits, and viruses and security patches.

2. References. The following references are available on the Job Corps Community Website (JCCW) at http://jcweb.jobcorps.org/documents/docu.htm.

- Program Instruction No. 02–20 LAN WAN Rules of Behavior
- Program Instruction No. 02–22 Authorized and Secured Data Circuits at Job Corps Centers
- JCDC Notice No. 02–231b LAN WAN Rules of Behavior
- JCDC Notice Nos. 04–51a, 04–51b LAN WAN Rules of Behavior
- JCDC Notice No. 04–103 Critical Security Update for Internet Explorer – UPDATED
- JCDC Notice No. 04–134 Windows Operating System Security Update Mandated

- JCDC Notice No. 04–136 Security Software Installation for IT POCs
- Job Corps Network IT and Security Policies and Procedures (attached)

3. Background. Over the past several years, Job Corps has worked toward centralizing data services for all its customers. The Citrix/Active Directory/Exchange environment is a central platform providing Job Corps network customers with access/authentication services, email, and office automation applications. As Job Corps continues to transition to a centralized data services model, several policies must be established and others reiterated.

a. Windows 95/98/2000/XP. There are approximately 20,000 devices (personal computers [PCs] and printers) that connect to the Job Corps network, including approximately 11,500 that were not purchased by the Department of Labor (DOL) but were provided through other sources. The Job Corps Data Center (JCDC) is responsible for providing upgrades and licensing only for those PCs provided by DOL. Licensing for other PCs must be provided by the center. However, Job Corps policy states that all PCs attached to the Job Corps network must be running Windows XP Professional (XP Pro) with Service Pack 2 installed (JCDC Notice 04–103, 04–134) because this upgrade to Windows XP Pro is required for Job Corps to remain in compliance with Federal policies. Therefore, the National Office of Job Corps provided a 6-month grace period starting December 8, 2004, for operators to upgrade the rest of the PCs on the network.

Rollout of thin clients to the Job Corps network will replace many of the older, non-compliant machines with machines that adhere to the Job Corps policy. Thin clients are less susceptible to hardware failures, viruses, theft, and configuration errors, and they are significantly less expensive than PCs. Thin clients also can be managed and maintained from a central console. This transition has been funded and begun at pilot Job Corps centers, creating a thin client Job Corps Student Network. The ultimate rollout of thin clients to all Job Corps centers will take place over the next several years.

b. Hubs and Unauthorized Wireless Access Points. Job Corps Policy states that no hubs or unauthorized wireless access points are to be connected to the Job Corps network (Program Instruction 02–20 and JCDC Notices 02–231b, 04–051, 04–051a, and 04–051b).

However, hubs and unauthorized wireless access points have been determined to exist on a significant number of Job Corps Local Area Networks (LANs). All hubs and unauthorized wireless access devices must be removed from Job Corps LANs immediately. Failure to remove the devices could result in discontinuation of network services until the unauthorized devices have been removed from the network.

c. Third-party Circuits. According to Job Corps policy (Program Instruction Notice No. 02–22), unauthorized third-party circuits must be disconnected immediately. They can be used to circumvent Job Corps Internet security policies and are a significant security concern, being a "back door" to the Job Corps private network. Note that third-party circuits are only allowed if a signed Memorandum of Understanding is on file between the center and the National Office of Job Corps.

Failure to disconnect any unauthorized third-party circuits may result in disconnection from the Job Corps network.

d. Viruses and Security Patches. It is imperative that all systems that connect to the Job Corps network have the appropriate virus signature files, the latest security patches and that the user takes precautions to prevent unauthorized access to Job Corps computers. Job Corps policy states that all systems connected to the Job Corps network must have anti-virus software loaded and up-to-date with the latest signature files and that all PCs must be updated with the latest security patches on a regular basis (JCDC Notices 04–051, 04–051a, and 04–051b). The anti-virus client has been made available to all center Point of Contacts (POCs) for download, with instructions for setting the PCs to auto-download virus signature file updates.

To combat viruses and security threats, the Job Corps technical team implemented the use of the Business Oriented Software Solutions (BOSS) Automated Security Patching software, requiring that it be installed on all PCs on the Job Corps network (JCDC Notice 04–136). Additionally, the Job Corps technical team is in the process of rolling out the Cisco Security Agent (CSA), a host-based intrusion detection software package on every PC in the Job Corps network. The CSA detects unusual activity at the local PC level and stops the activity based on a user profile and a set of configured rules that reside on a central server. CSA will prevent a virus-infected PC from infecting other PCs on the network.

4. Compliance. To comply with the existing Job Corps policies regarding the Job Corps network, POCs are required to perform the following tasks:

a. Remove all hubs and unauthorized wireless access points from the Job Corps network;

b. Disconnect all third-party circuits from the Job Corps network;

c. Install the provided antivirus software on all PCs that attach to the Job Corps network and configure the software for auto-update of its virus signature files;

d. Install the BOSS software on all PCs that are attached to the Job Corps network. The Job Corps technical team also recommends that POCs and Center Directors review the established Job Corps network policies outlined in the Attachment: Job Corps Network IT and Security Policies and Procedures.

e. Participate in training sessions offered by the JCDC on how to perform the above tasks. Training schedules will be provided at a later date and will also be available on the Training Web Site calendar at http://training.jobcorps.org/training.htm

4. Action. Addressees are to ensure that a copy of this Notice is distributed to the appropriate staff.

5. Expiration Date. Until superseded.

6. Inquiries. Inquiries should be directed to Gregg Colvin at colvin.gregg@jobcorps.org, Lori McElroy at mcelroy.lori@jobcorps.org, or to Linda Estep at Estep.Linda@dol.gov