November 1, 2007

DIRECTIVE: JOB CORPS INFORMATION NOTICE NO. 07-13

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: Two-Factor Authentication and Encryption of Job Corps Information Technology Systems

1. Purpose. To inform the Job Corps community about Office of Management and Budget (OMB) mandate M-06-16 and how it will affect remote access to Job Corps information technology (IT) systems.

2. Background. In 2006 the OMB issued M-06-16 (www.whitehouse.gov/**omb**/memoranda/fy2006/**m06-16**.pdf), which establishes requirements for remote access to government IT systems. The National Office of Job Corps has determined that OMB M-06-16 will guide how Job Corps users access Job Corps IT systems from outside the Job Corps private network.

a. OMB outlines security precautions that are to be implemented to help protect personally identifiable information (PII). These security precautions include the following:

(1) Encrypt all data on mobile computers/devices that carry Job Corps agency data unless the data is determined to be non-sensitive, in writing, by the Deputy Secretary or an individual he or she may designate in writing.

(2) Implement protections for PII being transported and/or stored off-site.

(a) Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

(b) Agency data may only be stored on government-issued equipment.

b. Job Corps has determined that there are two types of remote users of Job Corps systems:

(1) Users who access Job Corps IT systems from outside the Job Corps private network and require the ability to upload or download data to storage media local to their personal computer (PC) or laptop. (Storage media is defined as any device that can store data of any type, e.g., hard drive, USB drives, CD/DVDs).

(2) Users who access Job Corps IT systems from outside the Job Corps private network but do not require the ability to upload or download data to local storage media.

c. Job Corps has determined that Outreach and Admissions (OA) counselors and Career Transition Services (CTS) specialists are the primary users who require the ability to retain data on local storage media.

3. Definitions of Terms. For the purposes of this directive, the terms *full disk encryption, removable media encryption,* and *two-factor authentication* are defined as follows:

a. Full disk encryption refers to the encryption of all data on a hard disk, with the encrypted data on the hard disk accessible only to an individual with the correct credentials.

b. Removable media encryption refers to encryption of data that resides on media that may be removed from a PC or laptop without affecting the operation of the system. Examples of removable media include USB drives, DVDs, and/or CD-ROMs.

c. Two-factor authentication refers to an authentication method whereby a user is granted access to an IT resource through something the user knows, such as a password or personal identification number (PIN), and something they have, such as a token or smart-card that generates one-time passwords.

4. Action.

a. OA/CTS Personnel Access.

In order to comply with OMB mandate M-06-16, Job Corps will issue laptops with full disk encryption, removable media encryption, and two-factor authentication to all OA/CTS personnel.

(1) The National Office will **only** provide laptops to current OA/CTS personnel. This project does not include the purchase or deployment of desktop PCs, printers, or other peripheral devices.

(2) The laptops to be provided to OA/CTS personnel will come with a standardized Job Corps image inclusive of the Microsoft Office 2007 Suite and other common business software tools.

(3) OA/CTS personnel who are located outside the Job Corps private network will be required to access the Job Corps IT resources and applications through an SSL VPN (Secure Sockets Layer virtual private network) tunnel and use two-factor authentication in the form of an RSA token and PIN.

(4) Systems accessing Job Corps IT resources and applications through an SSL VPN will be scanned to determine if the system was issued by the Department of Labor, Office of Job Corps. If the system is validated as issued by DOL/OJC, then the system will be scanned to determine if full disk encryption, removable media encryption, Cisco Trust Agent, Cisco Security Agent, Anti-Virus client, virus signature files, and current OS patches are installed. If a system is determined to be deficient, the user will be redirected to a remediation Web page where the system can be updated with the required software, signature files, and/or operating system patches.

(5) The following steps will take place when a remote user connects through the SSL VPN:

(a) User will open a secure Web site.

(b) VPN Concentrator validates that the system was issued by DOL/OJC.

(c) VPN Concentrator validates system requirements (PointSec Disk encryption and removable media encryption, CTA, CSA, AV, etc.)

(d) User is prompted to enter user ID, PIN, and authentication code.

(e) Two-factor authentication appliances validate user and grant access to Job Corps IT resources with the ability to download or upload to and from an encrypted local storage medium.

(6) Removable Media Encryption.

(a) As stated previously, removable media encryption refers to the encryption of data that is transferred to removable media devices such as USB hard drives or CD/DVDs.

(b) OMB mandate M06-16 also specifies that removable media encryption must be installed on all PCs and laptops that are resident on the Job Corps private network.

(c) The Job Corps Data Center will push out removable media encryption to all PCs and laptops that reside on the Job Corps network. Please note that thin clients are exempted from this requirement.

(d) PointSec removable media encryption will encrypt data transferred to removable storage. The data transferred to the removable media may be shared as long as the originating user sets a password and provides that password to the receiver of the data.

(e) The Job Corps Data Center will "push" out removable media encryption to end user PCs through Network Admission Control. Removable media encryption will be required to be installed on the PC in order to access network resources.

(7) Status and Deployment.

(a) JCDC is currently building the back-end environment to support two-factor authentication and encryption, and is currently procuring the laptops and licensing required for this project.

(b) JCDC is developing a deployment schedule based on current active OA/CTS users and contracts, and will provide the deployment schedule to the Job Corps community as soon as it is complete.

(c) JCDC will contract with an integrator to image the laptops and drop ship the appropriate number of laptops to each OA/CTS location.

(d) Documentation regarding the initial laptop setup and two-factor authentication will be supplied to OA/CTS users.

(e) Deployment assistance will be available through a dedicated support group within the JCDC Technical Assistance Center.

(f) JCDC will also provide a schedule for deployment of removable media encryption.

(8) Training.

(a) JCDC is currently developing training documents for full disk encryption, removable media encryption, RSA two-factor authentication, and other related support documentation.

(b) JCDC will also host spotlight trainings for each of these topics.

(c) JCDC will provide a schedule for spotlight training to inform users, when it is available.

b. Non-OA/CTS Remote User Access.

Job Corps will continue to allow remote access to users who do not have a requirement to store data on local media resources.
Non-OA/CTS users will continue to have remote access to the Job Corps IT data and resources through Citrix by opening a Web browser and navigating to https://access.jobcorps.org. However, remote non-OA/CTS users will **not** have the ability to save, print, or capture screen shots of Job Corps data to a local storage medium (local hard drive, USB drive, etc.) unless RSA 2 factor authentication and Point Sec encryption has been installed on the remote equipment. Job Corps will be providing more information on the security tools and installation process.

Addressees are to ensure that this Information Notice is distributed to all appropriate staff.

5. Expiration Date. Until superseded.

6. Inquiries. Inquiries should be directed to the JCDC Help Desk at helpdesk@jobcorps.org or (800) 598-5008, or Linda Estep at estep.linda@dol.gov.