May 8, 2013

DIRECTIVE: JOB CORPS PROGRAM INSTRUCTION NO. 12-30

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: ROBERT W. PITULEJ
                  Acting National Director
                  Office of Job Corps

SUBJECT: Security Policy for Digital Dental X-ray Imaging Systems

1.   Purpose. To remind the Job Corps community of the security policy for digital dental
X-ray imaging systems.

2.   Background. Personally Identifiable Information (PII) is any information that can be
used to distinguish an individual's identity (e.g., name, Social Security number, date of birth,
etc.), and any other information that can be linked to an individual (medical, educational,
financial records, etc.).

        The dental X-ray images Job Corps collects from students are considered PII, and as
such, are protected by the Health Insurance Portability and Accountability Act of 1996, and the
Privacy Act of 1974. As the loss or unauthorized viewing of PII can have serious consequences
(identity theft, fraud, embarrassment to the individual), Job Corps takes the responsibility of
protecting student PII very seriously. Job Corps allows the use of digital dental X-ray imaging
systems, but requires that security precautions are followed in order to protect the students' PII
collected by the system.

        Job Corps' minimum requirements for securing digital dental X-ray imaging systems are
as follows:

   •   The system must be stand-alone, i.e., not connected to the internet or to the Job Corps
        network. Isolating the system protects it from the risks posed by network-related
        attacks.
   •   The system must be password-protected, and access must only be given to individuals
        who require it. Password-protecting the system reduces the likelihood of an
        unauthorized individual gaining access.

- The system must be kept in an area with restricted and protected physical access. Physically protecting the system (storing in a locked room and/or in a building with limited access and security camera monitoring) reduces the likelihood of theft.

Digital X-ray images must not be stored. They must be printed, placed in the student's medical folder, and then the digital copy must be deleted. Storing the images in their printed form rather than storing the images digitally on the system reduces a potential threat if the system is compromised.

3. <u>Action</u>. Job Corps centers should not store student digital dental X-ray images. Student digital dental X-ray images should be printed and placed in the student's medical folder. The digital copy should be deleted. Job Corps centers should also ensure that digital dental X-ray imaging systems are properly secured.

Addressees are to ensure this Program Instruction is distributed to all appropriate staff.

4. <u>Expiration Date</u>. Until superseded.

5. <u>Inquiries</u>. Inquiries should be directed to Carol Abnathy at (202) 693-3283 or abnathy.carol@dol.gov or Johnetta Davis at (202) 693-8010 or davis.johnetta@dol.gov.