Attachment B

US DEPARTMENT OF LABOR

Office of Job Corps

Job Corps: Protecting Personally Identifiable Information (PII) Policies and Procedures

Table of Contents

Introduction

This policy is taken, in part, from the U. S. Department of Labor Manual Series Chapter 1200 – Safeguarding Personally Identifiable Information and Other Sensitive Data. This is the governing authority providing direction for Job Corps implementation of an internal policy for safeguarding personally identifiable information (PII).

Purpose

This policy establishes guidance and responsibilities for the safeguarding of personally identifiable information (PII) and other Job Corps sensitive data that is accessed, processed, transported, or stored on end-user computing devices and portable media.

Scope

The policy guidance and responsibilities contained in this document apply to:

- All data held, used, or owned by Job Corps or the Department of Labor (DOL), including data that has been provided to, or supplied by, federal, state and local government partners and private sector partners in the conduct of DOL business;
- All Job Corps information systems and the data they contain; and
- All Job Corps staff and contractors.

Policy

It is Job Corps policy to ensure consistent, agency-wide compliance with Office of Management and Budget (OMB) mandates and all Federal legislation applicable to the protection of PII and other sensitive data.

Background

Federal Agencies are required to take aggressive measures to mitigate the risks associated with the collection, storage and dissemination of PII and other sensitive data. On May 22, 2006, OMB issued M-06-15, *Safeguarding Personally Identifiable Information.* In this memorandum, OMB directed Senior Officials for Privacy to conduct a review of Agency policies and processes and to take necessary corrective action to prevent intentional or negligent misuse of, or unauthorized access to PII.

This action was followed by a June 23, 2006 Memorandum (OMB M-06-16), in which OMB issued specific recommendations to Agencies on how to protect their sensitive data to be in compliance with security controls from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*.

On July 12, 2006 OMB issued M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*. In this memorandum, OMB provided updated guidance for reporting of security incidents involving PII.

Definition of PII

Personally Identifiable Information (PII). As defined by Office of Management and Budget (OMB) Memorandum M-06-19, July 12, 2006, PII means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

For purposes of this policy, Job Corps makes these distinctions:

Non-Sensitive PII. PII whose disclosure cannot be expected to result in personal harm. Examples include first/last name; e-mail address; business address; business telephone; general education credentials; and badge or identification number. This definition may apply to electronic documents (e.g. e-mail messages, electronic media, digital copies, etc.) generated or received by Job Corps system users. (See **Sensitive Data**, below, for caveats on handling of electronic documents.)

Protected PII**.** PII of a sensitive nature whose disclosure could result in harm to an individual. Examples include, but are not limited to, social security number; credit card number; bank account number; residential address; residential or personal telephone; biometric identifier (image, fingerprint, iris, etc.); date of birth; place of birth; mother's maiden name; criminal records; medical records; and financial records.

Definitions

Authentication. The process of verifying the authorization of a user, process, or device, usually as a prerequisite for granting access to resources in an Information Technology system.

Authentication Token. Something (usually a small device) that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity. Examples of tokens include smart cards; something embedded in a commonly used object such as a key fob; secret keys, private keys or a one-time password.

Designated Approving Authority (DAA). The senior agency management official who is responsible for ensuring that all agency information (major application or general support systems) are authorized to operate in accordance with certification and accreditation procedures established by the Chief Information Officer (CIO). The DAA is the agency head or designee.

Encryption. The process of changing plaintext into ciphertext for the purpose of security or privacy.

FIPS 140-2 Compliance. Refers to products with cryptographic modules that have been tested and validated as meeting the requirements of FIPS 140-2. The cryptographic validation program was established by NIST and the Communications Security Establishment in 1995. U.S Federal organizations must use validated cryptographic modules.

Information System. A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

Portable Media. Transportable devices that are capable of storing information. Examples of portable media are laptops, personal digital assistants (PDAs), and removable storage media such as USB drives, external hard drives, optical drives, CDs, and DVDs.

Portable System. A transportable device having an operating system. Laptops, PDAs, Blackberries and smart phones are examples of portable systems.

Remote Access. The ability to log onto a network from an external location, usually from outside the firewall. Generally, this implies a computer, a modem or other communication link, and remote access software to connect to the network.

Sensitive Data. Information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission; proprietary information; records about individuals requiring protection under the Privacy Act; and information not releasable under the Freedom of Information Act. For Job Corps purposes, this includes any information, which through loss, unauthorized access, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy of individuals (which is protected under the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This definition is not intended to

comprise all electronic documents (e.g. email messages, electronic media, digital copies, etc.) generated or received by Job Corps system users. Sensitive data contained in electronic documents shall be protected in accordance with the level of risk posed, as documented in the system's risk assessment.

Users. Persons who have been authorized to access Job Corps information, information systems, or information systems provided for Job Corps use under contract, subcontract, or other agreement.

USB or "thumb" Drive. Portable USB devices are devices used to store data and can be used to transfer data between other devices that have a USB port. These devices are also called "thumb drives, flash drives, pen drives, jump drives, etc…" They are typically small, lightweight, removable and rewritable.

Procedures for Safeguarding PII

Authorization to Access PII and Other Sensitive Data

Only personnel authorized by appropriate Job Corps Agency management shall have access to protected PII and other agency sensitive data, and only to the extent required to perform their duties and job responsibilities. Further, the Designated Approving Authority (DAA) must authorize all data sharing of protected PII that is governed by Memorandums of Understanding (MOUs), Interagency Agreements (IAs) and associated Interconnection Security Agreements (ISAs).

Usage of PII and Other Sensitive Data on Job Corps Equipment

Any information technology device (mobile or stationary) used to access or store protected PII and other sensitive data must be the property of the government and must be configured to meet the requirements of this and other applicable policies. Should a demonstrable business need exist to use contractor-owned computers for storage or for remote/mobile access to a Job Corps system containing such data, written authorization must be obtained from the DAA. Such authorization must be contingent on the contractor's equipment meeting the requirements established in the Job Corps Access Control Procedures.

Use of personally owned or public computers to handle or store protected PII and other sensitive data is prohibited.

Portable Media

Usage of PII and Other Sensitive Data on Portable Media

Protected PII or other sensitive data shall only be stored on portable media when absolutely necessary to meet business requirements, and only for the duration of the

specific business assignment for which the data is required. The storage of protected PII or other sensitive data on portable media devices must meet the minimum encryption standards described below.

Portable and mobile devices (e.g., notebook computers, workstations, personal digital assistants, USB or "thumb" drives) are not permitted access to Job Corps or DOL networks without first meeting the applicable security policies and procedures. Security policies and procedures include such activities as scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless).

Use of any portable device or media without encryption must be approved in writing by the Deputy Secretary of Labor or his/her designee. The data on the portable device or media must be determined, in writing, to be non-sensitive before approval will be granted by the Deputy Secretary or his/her designee.

Protection of Portable Media Devices and Their Data

Protected PII and other sensitive data on portable media devices issued by Job Corps must be protected with encryption. Portable devices with an operating system, such as laptops, require full device encryption, preferably at Basic Integrated Operating System (BIOS) level (i.e., activated during boot-up). All removable storage media, such as flash drives, USB or "thumb" drives, CDs, DVDs, writable optical media, and external hard drives that will store PII or other sensitive data, must be encrypted also.

All reasonable measures shall be taken to ensure that portable media containing protected PII and other sensitive data are stored inside a safe or in a secured, locked cabinet, room, or area during periods when the media is not in transit or in active use.

Portable Media Encryption Requirements

All selected encryption products at Job Corps must use FIPS 140-2-validated cryptographic modules operating in approved modes of operation. The encryption must be performed at the BIOS level or sometimes called "full disk encryption." The minimum encryption standards for these devices must follow encryption meeting the FIPS 140-1/2, Level 2 {Triple Data encryption Standard (3DES) or Advanced Encryption Standard (AES)}.

Transportation of Portable Media Containing PII or Other Sensitive Data

Portable media containing protected PII or other sensitive data may be transmitted by the United States Postal Service or another Job Corps-authorized delivery service if media is encrypted to Job Corps standards and double-wrapped in an opaque package or container that is sufficiently sealed to prevent inadvertent opening and to show signs of tampering. The package must be insured and registered with an ability to track pickup, receipt, transfer, and delivery. Consult the Job Corps Media Protection Procedures for additional protections that may be required depending on data sensitivity.

Sanitization or Destruction of Portable Media Containing PII or Other Agency Sensitive Data

Portable media containing protected PII or other sensitive data shall be sanitized or destroyed before disposal or release for reuse, in accordance with Job Corps Media Protection Procedures. All removable storage media, such as flash drives, USB or "thumb" drives, CDs, DVDs, writable optical media, and external hard drives that contains PII or other sensitive data must be destroyed using approved Job Corps sanitization techniques.

Marking of PII and Other Sensitive Data

All documents containing protected PII or sensitive information, including (but not limited to) spreadsheets, presentations, reports, word processing documents, and other computer-generated output must contain the designation of For Official Use Only or Sensitive Unclassified on each page of the output. Labels must be affixed to magnetic media that contains PII.

Use of E-mail and File Transfer Protocol (FTP)

Users are prohibited from using e-mail or FTP to transmit protected PII or other sensitive data outside of Job Corps firewalls unless such data is protected in accordance with Job Corps policies.

Remote Access to Job Corps Systems

Use of personally owned or public computers to access Job Corps protected PII is prohibited. All remote access to the Job Corps network must be initiated through an encrypted tunnel (VPN) or other encrypted mechanism such as Citrix or SSL. A remote access connection to Job Corps PII and other sensitive data should not be made through an unsecured wireless network. Remote access connectivity to protected PII and other sensitive data must be protected using a secure encrypted channel that is certified as FIPS 140-2 compliant.

Job Corps remote access systems must be configured to prevent caching of protected PII and sensitive information. In addition, all implementations that allow

remote access shall be configured to prevent copying and downloading of such data unless authorized in writing by the DAA and required for business reasons.

All implementations of remote access and mobile devices must employ a "time-out" function requiring user re-authentication after thirty minutes of inactivity. Job Corps has implemented a timeout value of 15 minutes for all remote access.

Two-Factor Authentication

All remote access to Job Corps systems must be authenticated using at least two factors. One of the two factors must be separate from the computing device, and will consist of a hardware authentication device that generates a one-time authentication code every 60 seconds or with every failed authentication attempt.

Logging and Verification of Data Extracts

Computer-readable data extracts from databases holding protected PII and sensitive information must be logged following the procedures established in the Job Corps Audit and Accountability Procedures. Each extract must be verified to ensure that such data either is erased within ninety days or is still required for use.

Penalties and Remedies

The Privacy Act of 1974 provides for both criminal penalties and civil remedies. Criminal penalties apply to individual employees, and civil remedies apply only to the Department.

A. Criminal Penalties

(1) Any Job Corps official or employee "who, by virtue of employment or position, has possession of or access to any Agency records that contain individually identifiable information, the disclosure of which is prohibited by the Act or by rules or regulations established there under, and who, knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or Agency not entitled to receive it, shall be guilty of a misdemeanor and be fined not more than $5,000."

(2) Any Job Corps official or "employee who willfully maintains a system of records without meeting the notice requirements" of prior publication in the *Federal Register* "shall be guilty of a misdemeanor and be fined not more than $5,000."

(3) "Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and be fined not more than $5,000."

B. Civil Remedies. If the Department fails to comply with provisions of the Act and a court determines that the failure is intentional or willful and had an adverse effect on an individual, the United States is liable to the individual in an amount equal to the sum of actual damages, but not less than $1,000, and costs of the action together with reasonable attorney fees as determined by the courts.

Authorities

- Privacy Act of 1974 (5 U.S.C. § 552a).
- Paperwork Reduction Act of 1995. (44 U.S.C. §§ 3501-3520).
- E-Government Act of 2002 (P.L. 107-347, 44 U.S.C. Chapter 36).
- OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 17, 2006.
- OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 12, 2006.
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006.
- OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, May 22, 2006.
- OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy, February 11, 2005.
- OMB Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 30, 2003.
- OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy, December 20, 2000.
- OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites, June 22, 2000.
- OMB Memorandum M-99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records," January 7, 1999.
- President's Memorandum on Privacy and Personal Information in Federal Records, May 14, , 1998.
- National Institute of Standards and Technology (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems, February 2005.
- DOL Computer Security Handbook 2006, Vols. 1-19.

- DOL Computer Security Incident Response Capability Guide.
- DLMS 5 – Chapter 200 – The Privacy Act of 1974 and Invasion of Privacy, November 17, 2004.
- DLMS 9 – Chapter 400 – Security, September 4, 2001.
- DLMS 9 – Chapter 1208 –Appropriate Use of DOL Information Technology, June 23, 2000.
- DLMS 9 – Chapter 1500 – Privacy Policy on Data Collection Over DOL Web Sites, December 22, 2000.
- DLMS 9 – Chapter 1200 –Safeguarding Personally Identifiable Information and Other Sensitive
- DOL Cyber Security Program Plan.