

**MEMORANDUM OF UNDERSTANDING
BETWEEN
U. S. DEPARTMENT OF LABOR
AND
NATIONAL COUNCIL OF FIELD LABOR LOCALS
(NCFL)**

INTRODUCTION

This Memorandum of Understanding (MOU) is entered into between the U. S. Department of Labor (DOL) and the National Council of Field Labor Locals (NCFL) in accordance with the applicable provisions of the master DOL-NCFL Agreement.

SUBJECT

This MOU concerns the impact and implementation of the Department of Labor Manual Series 9, Chapter 1200 (attached). This document establishes guidance and responsibilities for safeguarding sensitive data, including personally identifiable information (PII) that is accessed, processed, transported, or stored on end-user computing devices and portable media.

BACKGROUND

The Department shared with the National Council of Field Labor Locals, (NCFL) Department of Labor Manual Series (DLMS) 9 Chapter 1200, Safeguarding Sensitive Data Including Personally Identifiable Information. It is understood that the NCFL will retain all rights afforded by the provisions of Article 2 and Article 4 of the parties Collective Bargaining Agreement with regards to policies and procedures developed as result of the implementation of this DLMS Chapter.

TERMS OF THE AGREEMENT

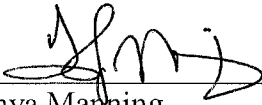
The parties agree to the following:

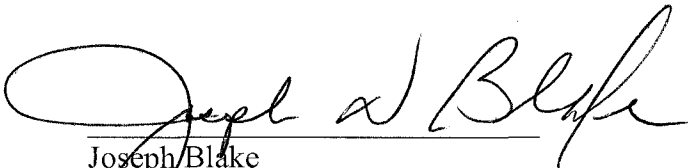
1. The parties agree that DLMS-9, Chapter 1200-Safeguarding Sensitive Data Including Personally Identifiable Information is applicable to both automated and manual/ paper-based information.
2. NCFL bargaining unit employees are encouraged to know the wireless interface policies of the agencies whose systems they use.
3. Agency designated approving authority authorization for remote access will satisfy the requirements of Section 1209.
4. By virtue of complying with the federal mandates for encryption, all encryption technologies implemented at DOL will be FIPS 140-2 compliant when deployed.

5. Users will not be held responsible for configuring remote access systems for compliance with Section 1216.
6. NCFLF bargaining unit employees will be held responsible only for those portions of the "System Security Plans" to which they have been given access. DOL agencies are responsible for providing employees access to the "Rules of Behavior" for the system(s) that they use.
7. In accordance with Section 1220 K. of the DLMS, agencies within the Department may develop policies concerning notifications in the event of the loss or theft of a portable media device containing PII.
8. NCFLF bargaining unit employees will be provided access, via LaborNet and/or RegionNet, to all authorities and references owned by the Department with regard to DLMS 9-1200. All other authorities and references are available via the Internet.
9. The Department will develop a training course specific to the requirements outlined in DLMS 9-1200. NCFLF bargaining unit employees will be afforded a reasonable amount of time to complete the training during normal work hours.

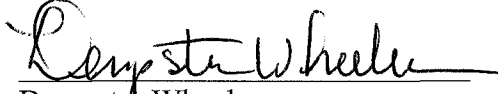
FOR THE DEPARTMENT

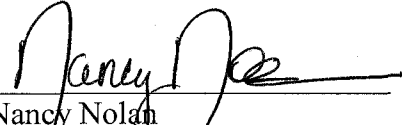

Yann King
Deputy Director
Information Technology Center

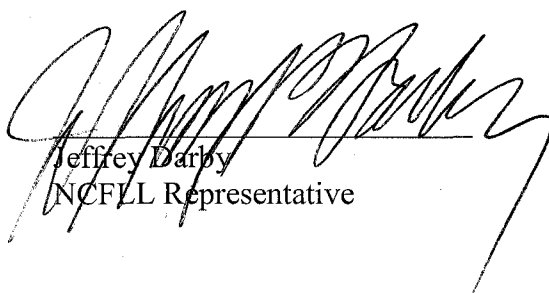

Tonya Manning
Chief Information Security Officer

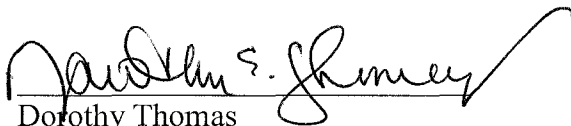

Joseph Blake
HR Specialist OELMR/OASAM

FOR THE NCFLF


Dempster Wheeler
Vice-President NCFLF


Nancy Nolan
Vice-President NCFLF


Jeffrey Darby
NCFLF Representative



Dorothy Thomas
HR Specialist OELMR/OASAM



Abraham Stern
NCFL Representative



Kevin O'Doherty
HR Specialist OELMR/OASAM

12/13/07

Date

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

1200 SAFEGUARDING SENSITIVE DATA INCLUDING PERSONALLY IDENTIFIABLE INFORMATION

1201 Purpose. This chapter establishes policy guidance and responsibilities for the safeguarding of agency sensitive data including personally identifiable information (PII) that is accessed, processed, transported, or stored on end-user computing devices and portable media.

1202 Scope. The policy guidance and responsibilities contained in this chapter apply to:

- All data held, used, or owned by the Department of Labor (DOL) for the purpose of DOL business, including data that has been provided to, or supplied by, federal, state and local government partners and the private sector in the conduct of DOL business;
- All DOL information systems (General Support Systems, Major Applications, and others);
- All information systems that store DOL information pursuant to a contract, subcontract, or other agreement;
- All DOL agencies, bureaus and offices, and users as defined in Section 1207.

This chapter is solely intended to prescribe safeguards for protecting sensitive information. It is not intended to set policy regarding the withholding or disclosure of sensitive data in litigation, under various statutes, or in response to court/tribunal requirements or orders, or congressional requests.

Nothing in this chapter shall limit in any way or otherwise contravene the authority or independence of the Office of Inspector General as set forth in the Inspector General Act of 1978, as amended.

1203 Policy. It is DOL policy to ensure consistent, department-wide compliance with Office of Management and Budget (OMB) mandates and all Federal legislation applicable to the protection of sensitive data. OMB has established requirements for Federal agencies that are reflected in this chapter. In addition, OMB anticipates that it will further refine or supplement its guidance pertaining to sensitive data and PII. Therefore, this chapter is subject to change as a result of future OMB guidance.

1204 Penalties and Remedies. The Privacy Act of 1974 provides for both criminal penalties against individuals and civil remedies against agencies.

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

- 1205 Background.** Federal Agencies are required to take aggressive measures to mitigate the risks associated with the collection, storage and dissemination of sensitive data including PII. 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. It established a Security Checklist, with action items, to ensure the implementation of OMB's recommendations. The Security Checklist action items were based on 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.

1206 Authorities and References.

- A. Civil Rights Act of 1964 (42 U.S.C. § 21) as amended.
- B. Rehabilitation Act of 1973 (29 U.S.C. § 701) as amended.
- C. Privacy Act of 1974 (5 U.S.C. § 552a).
- D. Paperwork Reduction Act of 1995. (44 U.S.C. §§ 3501-3520).
- E. E-Government Act of 2002 (P.L. 107-347, 44 U.S.C. Chapter 36).
- F. OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 17, 2006.
- G. 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.
- H. OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006.
- I. OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, May 22, 2006.
- J. OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy, February 11, 2005.
- K. OMB Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 30, 2003.

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

- L. OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy, December 20, 2000.
- M. OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites, June 22, 2000.
- O. 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.
- P. President's Memorandum on Privacy and Personal Information in Federal Records, May 14, 1998.
- Q. National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.
- R. *DOL Computer Security Handbook*, vols. 1-20.
- S. *DOL Computer Security Incident Response Capability Guide*.
- T. DLMS 2 – Chapter 1—DOL Property Management, May 3, 2005.
- U. DLMS 5 – Chapter 200 – The Privacy Act of 1974 and Invasion of Privacy, November 17, 2004.
- V. DLMS 9 – Chapter 400 – Security, February 15, 2007.
- W. DLMS 9 – Chapter 900 –Appropriate Use of DOL Information Technology, February 13, 2007.
- X. DLMS 9 – Chapter 1500 – Privacy Policy on Data Collection Over DOL Web Sites, December 22, 2000.

1207 Definitions.

- A. **Authentication.** The process of verifying the authorization of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.
- B. **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.
- C. **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.
- D. **Encryption.** The process of changing plaintext into ciphertext for the purpose of security or privacy.

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

- E. **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.
- F. **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.
- G. **Mobile Access.** The ability to access an information system without being physically connected to a network, usually with a portable device that has a wireless interface.
- H. **Personally Identifiable Information (PII).** As defined by OMB in Memorandum M-07-16 (May 22, 2007), “information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc..”

For purposes of this chapter, DOL makes these distinctions:

- I. **Non-Sensitive PII.** PII whose disclosure cannot reasonably be expected to result in personal harm. Examples include first/last name; e-mail address; business address; business telephone; and general education credentials that are not linked to or associated with any protected PII.
- J. **Protected PII.** PII whose disclosure could result in harm to the individual whose name or identity is linked to that information. 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. The conjunction of one data element with one or more additional elements, increases the level of sensitivity and/or propensity to cause harm in the event of compromise.
- K. **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.

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

- L. **Portable System.** A transportable device having an operating system. Laptops, PDAs, Blackberries and smart phones are examples of portable systems.
- M. **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.
- N. **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 DOL 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. This definition is not intended to extend to all electronic documents (e.g. email messages, electronic media, digital copies, etc.) generated or received by DOL system users. Sensitive data contained in electronic documents must be protected in accordance with the level of risk posed, as documented in the system's risk assessment.
- O. **Two-factor Authentication.** Any authentication protocol that requires two independent ways to establish identity and privileges. Common implementations of two-factor authentication use "something you know" (usually a password) as one of the two factors, and use either "something you have" (a token) or "something you are" (a biometric) as the other factor.
- P. **Users.** Persons who have been authorized to access DOL information, DOL information systems, or information systems provided for DOL use under contract, subcontract, or other agreement.

1208 Authorization to Access Sensitive Data

Users only have a right to access sensitive data to the extent necessary to perform their duties and assigned job responsibilities. Nothing in this chapter prohibits the Office of the Solicitor or the Office of the Inspector General from accessing sensitive data in order to carry out their responsibilities. Further, the DAA must authorize all data sharing of protected PII that is governed by Memorandums of Understanding (MOUs), Interagency Agreements (IAs), associated Interconnection Security Agreements (ISAs), and similar agreements.

1209 Usage of Sensitive Data on DOL Equipment

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

Any information technology device (mobile or stationary) used to access or store protected PII and other sensitive data must either be the property of the government or government-authorized or leased, and must be configured to meet the requirements of this and other applicable policies. Written authorization from the agency DAA is required in cases where use of government-owned equipment is not practical or possible. Cases requiring DAA authorization include, but are not limited to:

- Use of contractor-owned computers for storage or for remote/mobile access to a DOL system containing protected PII and other sensitive data;
- Use of personally owned or public computers to access, handle, or store such data in mobile workforce arrangements;
- Use of personally owned or public computers to access, handle, or store such data in emergency situations such as pandemic and contingency operations.

The DAA authorization of non-government equipment must acknowledge the DAA's awareness of and acceptance of the risks inherent in using such equipment; describe how the agency intends to mitigate those risks; and impose appropriate stipulations and rules of behavior. The DAA cannot authorize non-government equipment to access a system or application (e.g., universal applications) owned by another DOL agency, without the express approval of the owning agency.

1210 Usage of Sensitive Data on Portable Media

Protected PII or other sensitive data must only be stored on portable media when absolutely necessary to meet business requirements as determined by the system owner, and only for the duration of the specific business assignment for which the data is required.

1211 Protection of Media Devices and Their Data

Protected PII and other sensitive data on portable media devices issued by DOL 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) or Extensible Firmware Interface (EFI) level (i.e., activated during boot-up). All removable storage media, such as flash drives, CDs, DVDs, writable optical media, and external hard drives that will store protected PII or other sensitive data, must be encrypted. All selected encryption

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

products at DOL must use FIPS 140-2-validated cryptographic modules operating in approved modes of operation.

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. Agencies seeking an exemption to the encryption requirement must use the approval form as well as follow the process contained in the *DOL Computer Security Handbook*.

All reasonable measures will 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.

1212 Transportation of Portable Media Containing Sensitive Data

Portable media containing protected PII or other sensitive data may be transmitted by the United States Postal Service or another DOL-authorized delivery service if media is encrypted to DOL 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 decryption key must not be included in the same package, but transmitted via a separate or alternate channel. The package must be sent via certified carrier with an ability to track pickup, receipt, transfer, and delivery. Consult the *DOL Computer Security Handbook* for additional protections that may be required depending on data sensitivity.

In addition, such media may be transmitted by DOL interoffice mail provided it is double-wrapped to afford sufficient protection against inadvertent access.

1213 Use of E-mail and File Transfer Protocol (FTP)

Agencies are required to establish and enforce risk-based policies pertaining to the use of electronic mail or FTP to transmit protected PII or other sensitive data outside of DOL firewalls. Appropriate technologies such as public key cryptography and Secure FTP must be considered in cases where there is a documented business need to handle sensitive data via e-mail or FTP.

Agencies are encouraged to append a standard disclaimer notice to outgoing e-mail messages to notify recipients that the message, and any files transmitted with it, are confidential and intended solely for the use of the individual or entity to whom they are addressed; that the DOL sender should be notified if a message is

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

received by mistake; and that the unintended recipient is prohibited from disclosing, copying, or disseminating a message that is received in error.

Users are prohibited from using e-mail or FTP to circumvent the safeguards in this chapter pertaining to the transmission, use, and storage of protected PII and other sensitive data.

1214 Sanitization or Destruction of Portable Media Containing Sensitive Agency Data

Portable media containing protected PII or other sensitive data must be sanitized or destroyed before disposal or release for reuse, in accordance with the *DOL Computer Security Handbook*.

1215 Logging and Verification of Data Extracts

Computer-readable data extracts from databases holding protected PII or other sensitive information must be logged following the procedures established in the *DOL Computer Security Handbook*. Each extract must be verified to ensure that such data either is erased within 90 days or is still required for use.

1216 Remote Access to DOL Systems

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.

DOL remote access systems must be configured to prevent caching of protected PII and sensitive information. In addition, all implementations that allow remote access must 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 no greater than 30 minutes of inactivity.

1217 Two-Factor Authentication

All remote access to DOL 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.

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

Systems that, as of June 2007, already employ or have procured two-factor authentication (e.g., via smart card, biometric device, USB token, or time-synchronization device) are not required to change technologies. Remote access systems that do not currently use a hardware token are required to implement the solution described herein.

1218 Annual PII Report from Agency Heads

DOL agency heads are required to provide an annual report to the Office of the Chief Information Officer (OCIO) certifying that they have conducted a review of their processes, procedures, and systems to ensure that PII is protected by adequate security safeguards. Agency heads must conduct a review of the agency's inventory of systems that contain such information and confirm that security controls for its protection are properly implemented. This annual report must also include a review of the agency's access to and management of PII. The templates and schedule for the report will be provided to the agencies by the OCIO.

1219 Collection and Use of Social Security Numbers (SSNs)

For new information systems initiated subsequent to the issuance of this Chapter, agency programs shall collect, use, maintain, and disseminate SSNs only when required by statute. Absent this requirement, agency programs shall not collect or use an SSN as a unique identifier; rather, programs shall create their own unique identifiers to identify or link information concerning an individual.

1220 Responsibilities

The protection of PII and other sensitive data depends on the involvement of all DOL agencies and departmental offices that acquire, develop, operate, or replace information systems components. Agencies and offices must participate in the formulation and approval of DOL policies, implementation directives, requirements, procedures, and controls. Agencies, offices, and personnel must carry out responsibilities as follows:

- A. The **Deputy Secretary of Labor or his/her designee** must provide written authorization for the use of any portable device or media which carry non-encrypted DOL data that is determined to be non-sensitive, as required by OMB M-06-16.
- B. The **Chief Information Officer (CIO)** must develop and implement the department-wide program for protecting PII and other sensitive data and ensure that agencies are carrying out agency-wide programs. The CIO must issue additional policies, procedures, and guidance through other documents

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

such as, but not limited to, the *DOL Computer Security Handbook*. The CIO must carry out the following responsibilities:

- (1) Incorporate safeguards for the protection for PII and other sensitive data into DOL's Security Program.
- (2) In a collaborative manner with DOL agencies, develop and/or oversee development of the following as they relate to protected PII and other sensitive data:
 - (a) Information technology policies;
 - (b) Standards, plans, and guidance;
 - (c) Architectures and concepts of operation;
 - (d) Procedures, processes, and methodologies to ensure that all such information that is stored, disseminated, or transmitted by DOL-owned information systems or by other systems provided for DOL use under contract or subcontract is properly safeguarded against unauthorized access, use, modification, or destruction, through the integration of management, operational, and technical controls; and
 - (e) Independent verification and validation of the Agency Heads' annual PII report to ensure the protection of sensitive information (e.g., personal health information, financial information, etc.).
- (3) Ensure issuance of implementation directives in support of this chapter and in concert with DOL agencies.
- (4) Manage all DOL protected PII and other sensitive data program elements, including policy formulation, policy compliance, program evaluation, awareness, and threat analysis.
- (5) Require that agency heads provide an annual report certifying that the agency has conducted a review of processes, procedures, systems, inventory, security controls and access management to ensure that PII is protected by adequate security safeguards.
- (6) Ensure that all information system acquisition and contracting actions, including service life extension and decommissioning activities, comply with DOL policy as it pertains to protected PII and other sensitive data protection.

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable
Information

- (7) Ensure that protected PII and other sensitive data requirements and cost estimates are addressed in the DOL capital investment planning process throughout each system's life cycle.
- (8) In consultation with the Office of the Solicitor, oversee development of DOL procedures for managing access to protected PII or other information determined to be sensitive, including procedures that require:
 - (a) Review of the sensitivity of information entered, accessed, processed, transmitted, or stored on DOL information systems;
 - (b) Approval of new information systems, initiated subsequent to the issuance of this Chapter, which propose to collect, use, maintain, and disseminate SSNs.
 - (c) Issuance of guidelines regarding access to sensitive systems-based information;
 - (d) Issuance of guidance about how to apply personnel security requirements in accordance with federal laws and regulations;
 - (e) Consultation, as appropriate, with the Office of the Solicitor prior to the release of sensitive information.
- (9) Ensure risks and other implications resulting from technology or budget changes are communicated to DOL agencies and offices.
- (10) Ensure that DOL personnel receive adequate training in their responsibilities for protecting PII and other sensitive data.

C. The responsibilities of **Agency Heads** are as follows:

- (1) Comply with the requirements of the *DOL Computer Security Handbook* as they pertain to protected PII and other sensitive data.
- (2) Develop and implement information security procedures and mitigating controls sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of protected PII and sensitive information.
- (3) Assign duties to safeguard protected PII and other sensitive data to qualified agency personnel.

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

- (4) Include security requirements for protected PII and other sensitive data in the agency's IT capital investment planning and management process as required by the DOL Guide to IT Capital Investment Management.
- (5) Ensure that the requirements of the Privacy Act and other laws protecting sensitive information are incorporated into the Agency Computer Security Program.
- (6) Ensure that IT personnel, new employees and system users receive role-based training in protecting PII and other sensitive data.
- (7) Grant access to protected PII and sensitive information only to appropriate personnel (in accordance with applicable law or regulation, or DOL policies and procedures) who meet the requirements of the Agency's System Security Plans and comply with guidance provided by the CIO.
- (8) Address security requirements for protected PII and other sensitive data, and their associated cost estimates, in any DOL acquisition management system and throughout the life cycle for systems and services, including service-life extension and decommissioning activities.
- (9) Ensure that computer incident response capability is implemented for handling incidents involving the compromise or loss of protected PII and other sensitive data, in accordance with DOL policy, the *DOL Computer Security Handbook*, and NIST Special Publication 800-61, *Computer Security Incident Handling Guide*.
- (10) Ensure that all agency personnel, contractors, and subcontractors working for, or on behalf of, the agency take security measures commensurate with the sensitivity level of the data and the risk management required.
- (11) Apply measures to assure the confidentiality of protected PII and other sensitive information that is transmitted between geographically separated facilities.
- (12) Ensure that all remote access to systems employs two-factor authentication in accordance with this chapter and the *DOL Computer Security Handbook*.
- (13) Ensure that all portable media is equipped with the appropriate encryption technology in accordance with this chapter and the *DOL*

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

Computer Security Handbook. Where need exists to issue equipment without encryption, ensure that the affected data is non-sensitive, and that justification for the exception is appropriately documented and forwarded to the Deputy Secretary of Labor for his or her approval.

- (14) Ensure that the agency identifies, inventories, and reports to the CIO all portable systems within its control. An inventory and reconciliation of all portable systems and devices should be done at least annually as part of the Agency's requirement to inventory and reconcile all accountable property in accordance with Section 110 of DLMS 2-100, *DOL Property Management*.
- (15) Maintain and update the inventory of all agency information technology systems that contain sensitive data.
- (16) Certify in an Annual Report to the CIO that the Agency has:
 - a. Reviewed its processes, procedures, and systems to ensure that PII and sensitive information is protected by adequate security safeguards.
 - b. Reviewed its inventory of systems that contain PII and sensitive information and confirmed that security controls for the protection of this information are properly implemented.
 - c. Reviewed its access and management of PII and sensitive information.
- D. The **Solicitor of Labor** is responsible for providing legal advice and assistance for activities under this chapter.
- E. The **Chief Information Security Officer** is responsible for leading DOL Security Incident Response and managing all incident-related activities. These activities are as follows:
 - (1) Respond immediately to a reported incident of the theft or loss of a device containing PII (both protected and, as appropriate, non-sensitive PII such as first/last name) or other sensitive data and report to US-CERT within one hour of incident discovery.
 - (2) Coordinate with Office of the Inspector General, Department Senior Management, Office of the Solicitor, or other DOL or Federal agencies for the identification and investigation of any reported incident involving

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

the loss or theft of PII or other sensitive data as described in the *DOL Computer Security Handbook*.

- (3) Provide support as required to assist in reporting, tracking and resolving incidents that involve the loss or theft of PII.
 - (4) Coordinate DOL technical resources required for the identification and development of corrective fixes to incidents and vulnerabilities involving loss or theft of PII.
 - (5) Document and maintain all incidents and vulnerabilities involving loss or theft of PII that are reported under Departmental procedures and guidance.
 - (6) Develop, maintain and publish procedures required for handling incidents that involve portable media.
 - (7) Disseminate to all DOL agencies the lessons learned from specific incidents involving loss or theft of PII.
 - (8) Develop, maintain, update, and publish a template for annual reporting by Agency Heads on privacy and security information as outlined in Section 1219.
 - (9) Develop a written authorization process for the Deputy Secretary of Labor or his/her designee to approve the use of any portable device or media which carry DOL non-sensitive data without encryption as required by OMB M-06-16 and outlined in Section 1212.
 - (10) Maintain and update the inventory of all DOL IT systems that contain sensitive data.
 - (11) Facilitate, coordinate, and track computer security awareness and training for users as well as role-based training relative to PII usage and responsibilities.
 - (12) Carry out any other duties designated by DOL policy.
- F. The designated agency **Information Security Officers** are responsible for implementing and maintaining their agencies' information security program, applying DOL information security policy, leading their respective agency's Computer Security Incident Response Team (CSIRT) activities, and managing all incident activities at their agency's level, as follows:

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

- (1) Respond immediately to a reported incident involving PII (both protected and, as appropriate, non-sensitive PII such as first/last name) or other sensitive data. Report to DOL CSIRT within an hour of discovering the incident.
- (2) Coordinate with the DOL Chief Information Security Officer (CISO), the Office of the Inspector General and Agency Senior Management, and as directed by the CISO, coordinate with the Office of the Solicitor, or other Federal agencies for the identification and investigation of any reported security incident or of an individual or group of individuals responsible for compromising PII and other sensitive data.
- (3) Provide support to their agencies, as required, in reporting, tracking and resolving such incidents.
- (4) Coordinate their agencies' technical agency resources required for the identification/development of corrective fixes to incidents and vulnerabilities involving loss of theft of PII.
- (5) Document and maintain all security incidents and vulnerabilities involving loss or theft of PII that are reported under Departmental procedures and guidance.
- (6) Develop, maintain, and publish procedures required for their respective agencies in regards to the reporting and handling of portable media incidents.
- (7) Forward all Security Incident Advisories to individuals responsible for affected systems, and report actions to the CISO.
- (8) Carry out any other duties designated by DOL policy and DOL-approved agency policy.

G. The Director, Civil Rights Center, OASAM, must:

- (1) Apply the necessary internal controls and safeguards defined by applicable law to DOL sufficient to afford security protections to preclude unauthorized disclosure, modification, or destruction of protected PII and other sensitive information.
- (2) Require DOL grantees to take steps to establish policies and procedures that provide a reasonable guarantee of compliance to protect and safeguard PII and confidential information.

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

- (3) Ensure that the requirements of the Privacy Act and other laws protecting PII and sensitive information are incorporated into Equal Employment Opportunity training courses for DOL managers and supervisors.

H. The **Director, Human Resources Center, OASAM**, must:

- (1) Apply personnel program security procedures defined by applicable law to DOL personnel accessing information systems and sensitive data.

I. **Contracting Officers** must:

- (1) Include a statement in all contracts that, in addition to systems and information at DOL facilities, chapter DLMS 9-1200 applies to all non-DOL equipment and systems that store, process, or transmit DOL information.
- (2) Incorporate functional and assurance requirements for PII and other sensitive data in information system procurement documents in accordance with this chapter.
- (3) Require prime contractors, subcontractors, and grantees to comply with requirements of the DOL personnel security program as defined by applicable law, regulation, or policy, prior to accessing information systems or other assets determined to be sensitive.
- (4) Ensure that existing and future contracts involving IT information resources and portable media within the scope of this chapter comply with provisions of the Privacy Act and other legal requirements governing sensitive information.
- (5) Ensure that PII for contract employees is protected during the “enter on duty” and separation processes.

J. The **OASAM Departmental Budget Center** must:

- (1) Review all agency budgets to assure that the funds for protecting PII and other sensitive data are included.

K. **Users**:

Users must comply with this chapter and those of the following subordinate guides: *Cyber Security Program Plan*, *Agency Security Program Plans*, *System Security Plans*, and the *DOL Computer Security Handbook*. The term

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

“Users” as defined in section 1207-P. They must also apply the following DOL security practices to daily work activities:

- (1) It is the responsibility of individual users to protect the PII and other sensitive data to which they have access.
- (2) Users must adhere to the rules of behavior defined in applicable System Security Plans, DOL and agency guidance, and DLMS 9-1208, *Appropriate Use of DOL Information Technology*.
- (3) Users are prohibited from the unauthorized uploading, downloading, access, use, transmittal, copying, reproduction, erasure, or modification of information the Federal government deems to be sensitive or containing PII.
- (4) Users must not let other people see their passwords, and they must not keep a written copy of passwords.
- (5) Users must not allow anyone else to use or share their:
 - (a) User ID;
 - (b) Password;
 - (c) Cryptographic key;
 - (d) Digital certificate;
 - (e) Authentication token.
- (6) Users are responsible for complying with DOL computer security policies at all off-site locations such as residences when working in a Flexiplace arrangement.
- (7) In the event of the loss or theft of a portable media device containing PII (both protected and, as appropriate, non-sensitive PII such as first/last name) or other sensitive data, the user must immediately report the incident to his or her ISO and take any additional steps as instructed by the ISO.

L. **System Owners** are the individuals or entities responsible for establishing the rules for appropriate use and protection of the data and information within a system. They must:

DLMS - 9
INFORMATION RESOURCES
Chapter 1200 - Safeguarding Sensitive Data Including Personally Identifiable Information

- (1) Ensure that their systems, technical personnel, and users comply with all applicable legal requirements, including the Privacy Act, as well as their Agency's Computer Security Program Plan, the System Security Plan, and the *DOL Computer Security Handbook*.
- (2) Report portable media incidents in accordance with the System Security Plan, the Agency Computer Security Program Plan, and the *DOL Computer Security Handbook*. In addition, system owners must cooperate with incident response team members as guided by the Agency ISO and the DAA.

M. The **Designated Approving Authority** must:

- (1) Provide written authorization for the use of contractor-owned computers for remote or mobile access to a DOL system containing PII and sensitive data.
- (2) Follow the responsibilities outlined in the *DOL Computer Security Handbook*.
- (3) Authorize in writing all data sharing of PII that is governed by MOUs, ISAs, and IAs.
- (4) Request CIO approval prior to collecting, using, maintaining, or disseminating SSNs in any new information systems initiated subsequent to the issuance of this Chapter.
- (5) Provide written authorization for the use of personally-owned or public computers to access, handle, or store protected PII and other sensitive data.
- (6) Authorize in writing any remote access configuration that permits the copying/downloading of protected PII and other sensitive data.