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

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 (NCFLL) in accordance with the applicable provisions of the master DOL-NCFLL Agreement.

SUBJECT

This MOU concerns the impact and implementation of the Information Technology Center's (ITC) Office of Administration and Management (OASAM), Employee Computer Network (ECN) Portable Systems Equipment Policy (attached). This policy provides guidance and includes responsibilities for the appropriate use and security of Government Furnished Equipment (GFE) laptops and other portable devices used to access or work on the ECN. Agencies included in this policy are: Office of the Assistant Secretary for Administration and Management, Office of the Solicitor, Office of the Secretary, Office of Congressional and Intergovernmental Affairs, Office of Small Business Programs, Office of Public Affairs, Office of the Chief Financial Officer, Office of Disability Employment Policy, Office of the Assistant Secretary for Policy, Bureau of International Labor Affairs, Veterans' Employment and Training Service, and Women's Bureau.

BACKGROUND

The Department shared the ITC's OASAM/ECN Portable System Policy with the NCFLL. The parties enter into this MOU to achieve the most effective appropriate arrangement and procedures possible to serve the interest of bargaining unit employees.

TERMS OF THE AGREEMENT

The parties agree to the following:

1. The OASAM/ECN asserts that all portable government furnished equipment (GFE) will be compliant with OASAM/ECN Portable Systems Equipment Policy on the date the policy is implemented.
2. In the future, when a bargaining unit employee acknowledges receipt of portable GFE, OASAM/ECN will ensure that the equipment assigned to that employee is compliant with the OASAM/ECN Portable Systems Equipment Policy.

3. It is the intent of the parties to insure that implementation of this policy will have no negative impact on employee performance.

4. Portable GFE will be configured so that they do not prompt users to connect wirelessly.

5. Portable GFE users will be reimbursed for expenses incurred in contacting the ITC Help Desk in the event of loss or theft as described in the policy.

6. When a call is made to the ITC help desk for after hours support, and the on-call analyst does not answer, the caller will be directed to voicemail. The voicemail prompt will explain what information should be provided.

7. ITC requires the Help Desk Analyst to enter a ticket for each call that is received. The Help Desk Analyst will enter into ITC's call data base the date and time of each call for reports of loss or theft of portable GFE and media reported by ECN users. All tickets in the data base will be stored for at least a year. The user will receive an email confirming that their report has been received.

8. Portable GFE users will be provided a wallet card that provides instructions on how to contact the ITC help desk in the event of loss or theft and what information they should provide to the ITC help desk. Space will be provided for the user to enter their portable GFE serial number(s).

9. OASAM/ECN will provide cable locks and/or other security hardware. Bargaining unit employees will not be encouraged or required to personally purchase cable locks or other security hardware.

10. Employees will select the combination for their cable lock.

11. Management acknowledges that a cable lock cannot prevent all loss or theft. Management also acknowledges that hotel room safes may not be large enough to accommodate portable GFE.

12. Management will develop a concise handout that explains the OASAM/ECN Portable Systems Equipment Policy. This handout will include "best practices" to alert bargaining unit employees to alternative methods to ensure physical security of the portable GFE. This handout will be provided electronically to each bargaining unit employee who is assigned a portable GFE.

13. OASAM/ECN will provide E-mail reminders to all users to connect all portable GFE to the network at least every 30 calendar days. These reminders will be incorporated into the ECN technical announcements.

14. Bargaining unit employees will not be penalized for a breach of security resulting from lack of two factor authentication and/or encryption until such time that the OASAM/ECN implements these features. Notice of change detailing the proposed implementation of two factor authentication and encryption will be forthcoming to the NCFLL. The NCFLL may request negotiations if appropriate.

15. Management agrees to provide advance notice to the NCFLL of any change to this policy.

16. This Memorandum of Understanding will be distributed to all impacted bargaining unit employees.

FOR THE DEPARTMENT

Yann King
Deputy Director, Office of
Information Technology

Robert Behm,
OASAM Security Officer

Jacquelyn Coleman

Jacquelyn Coleman
Desktop Manager

Kevin O'Doherty
HR Specialist OELMR/OASAM

Joseph Blake

Joseph Blake
HR Specialist OELMR/OASAM

FOR THE NCFLL

Dempster Wheeler
Vice-President NCFLL

Dennis P. DeMay

Dennis DeMay
Vice-President NCFLL

Robert C. Tucker

Robert Tucker
Vice-President NCFLL

Julie Lowrie
NCFLL Representative

Steven Southwood
NCFLL Representative

June 28, 2007
Date

OASAM/ECN Portable Systems Equipment Policy

United States Department of Labor

Office of the Assistant Secretary for Administration and Management (OASAM)

Prepared By
OASAM

Information Technology Center
United States Department of Labor
200 Constitution Avenue, NW
Washington DC 20210

Version 1.2

June 28, 2007

DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
03/12/2007	Portable Systems Policy v1.0	Jacquelyn Coleman	Draft
04/16/2007	Portable Systems Policy v1.1	Jacquelyn Coleman	Final
06/28/2007	Portable Systems Policy v1.2	Jacquelyn Coleman	Rewrite

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers

Table of Contents

1. Background

There is a growing need to have federal employees perform their duties away from their official work location. Increased telework demands, support of Continuity of Operations Plans (COOP), Pandemic Influenza Response support, and official travel are just a few of the reasons why federal employees require portable Government Furnished Equipment (GFE) tools to perform their official responsibilities away from their permanent work location. In response to this need, the Information Technology Center (ITC) has begun to purchase more laptops in lieu of desktops. This policy addresses the Employee Computer Network (ECN) policies as it relates to portable systems that are used to access or work on the ECN. In the near future, this policy will be updated to address encryption of information on the portable systems, as well as two-factor authentication requirements for the ECN.

2. Purpose

This policy provides guidance and responsibilities for the appropriate use and security of GFE laptops and other portable remote devices used to access or work on the ECN. The Department of Labor (DOL) Computer Security Handbook (CSH) version 3 provides the parent policy.

3. Authority

The authority for this policy is the Department of Labor Manual Series (DLMS) 9, Chapter 400, Information Technology Security, DLMS 9 Chapter 1208, Appropriate Use of DOL Information Technology, DLMS 9 Chapter 1200, and DLMS 2 Chapter 100, DOL Property Management.

The most critical laws, regulations, Executive Orders, and directives pertaining to system and communications protection and the protection of information system resources are indicated below. References to the full list of statutes, federal regulations, directives, and National Institute of Science and Technology (NIST) publications applicable to Information Technology security in DOL are located in the Computer Security Handbook, Volume 21, Relevant Sources.

- 21 CFR 102-172, Federal Management Regulation, Telecommunications Management Policy
- Department of Labor Manual Series, September 4, 2001
- Department of Labor System Development Life Cycle Management Manual (SDLCMM), December 2002
- Federal Financial Management Improvement Act of 1996 (FFMIA)
- Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 2001
- Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003
- Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006

4. Definitions

Government Furnished Equipment (GFE). It is defined as any information technology equipment that the federal government issues to an employee. This includes, but is not limited to, laptops, desktops, blackberries, peripherals (printers, scanners, monitors, keyboards, mice, and docking stations), cell phones, and storage media such as thumb drives.

Personally Identifiable Information (PII). As defined by the 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.

Portable System. A transportable device having an operating system; laptops, personal digital assistants, blackberries and smart phones are examples of portable systems.

Portable Media. A floppy disk, CD, DVD, tape or flash memory drive that is plugged into a USB or FireWire port or a PC card slot on a laptop/desktop.

Remote Access. Is the ability to log onto a network from an external location, usually from outside the firewall. Generally, remote access consists of a computer, a modem or other communication link, and remote access software to connect to the network. NIST SP 800-53 provides this definition "Access by users (or information systems) communicating external to an information system security perimeter".

System Owner. A system owner is the individual who has been assigned ultimate responsibility for the end-to-end delivery of information and data, including all computerized processes and the hardware and software that are needed to satisfy business requirements.

Users. Persons who have been authorized to access ECN hosted information, ECN information systems, or information systems provided for DOL use under contract, subcontract, or other agreement; or an individual or (system) process authorized to access an information system.

5. Laptop Policy

5.1 Issuance

An employee may be issued a GFE laptop, or a GFE laptop with docking station, when his/her responsibilities include performing their duties away from their permanent duty stations such as in support of COOP Plans, Pandemic Influenza Response support, telework responsibilities, or other situations to remotely connect to the ECN. An employee is not typically allowed both a laptop and a desktop computer. Exceptions to a user requiring a laptop and desktop issuance must be approved by the appropriate OASAM Center Director/Regional Administrator or in the case of another agency on the ECN, the Agency/Office Supervisor. Non-GFE (including laptops) is not allowed to be connected to the ECN/DCN, in accordance with requirements as defined in NIST SP 800-53 and the DOL CSH version 3.

5.2 Physical Security

In accordance with requirements as defined in NIST SP 800-53 and the DOL CSH v3, Vol. 11, Physical and Environmental Protection, employees are responsible for the physical security of portable system GFEs. Users should not leave a laptop unattended for an extended period of time unless it is secured by a cable lock or other means to deter theft. Users should take adequate measures to protect portable systems GFE in the same manner as they would protect their own valuable personal electronics equipment.

5.3 Monthly Software Patches and Updates

In accordance with requirements as defined in NIST SP 800-53 and the DOL CSH v3, Volume 9, Maintenance (Specifically, NIST SP 800-53 Control MA-6), when laptops are connected to their ECN connected docking station, like typical ECN desktops, the laptop will receive periodic software updates and patches from the ECN when the user logs on to the ECN. However, when the laptop is not in the docking station or the user does not have a docking station, then a user must periodically connect the laptop to the ECN via the secure remote access capability, thus allowing the laptop to receive the necessary software patches and upgrades. It is essential that users connect their laptops to the ECN at least once every 30 calendar days in order to receive patches and updates. If an employee's laptop has not been connected to the network in over 30 calendar days, the ITC will discuss this oversight with the employee's supervisor. The supervisor will remind the employee of the requirement to connect to the network within 30 calendar days.

5.4 Procedures for Reporting Loss or Theft

Employees are required to report the loss or theft of portable systems to the ITC Help Desk at 202-693-4444, within thirty minutes of noticing the loss or theft. When calls are received during after hour support, the caller should press 1 to be routed to the "On Call" Analyst to receive immediate assistance. It is also the employee's responsibility to notify her/his supervisor of the incident.

This requirement is in accordance with NIST SP 800-53 and the DOL CSH v3, Volume 8, Incident Response, and OMB M-06-19, which requires agencies "to report all incidents involving personally identifiable information to US-CERT within one hour of discovering the incident. Employees should report all incidents involving personally identifiable information in electronic or physical form and should not distinguish between suspected and confirmed breaches."

5.5 Use of Sensitive Data on Portable Media

In all cases, users, to the maximum extent possible, should store all sensitive and PII information on the ECN shared drives and not on the hard drive of the laptop. 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.

5.6 Wireless Connectivity to the ECN

Currently wireless connectivity is disabled on GFE laptops. Enabling wireless capability on GFE laptops is strictly prohibited, in accordance with requirements as defined in NIST SP 800-53 and the DOL CSH version 3, Volume 1, Access Controls (Specifically, NIST SP 800-53 Controls AC-18 and AC-19)

6. Blackberry Use

Only government furnished devices are permitted for connectivity with the ECN. Issuance of blackberries must be approved by the OASAM Center Director or Regional Administrator or other authorized official. **Sections 5.2 Physical Security and 5.4 Procedures for Reporting Loss or Theft** above applies to use of blackberries on the ECN. User agencies are responsible for all costs associated with the blackberry, including monthly airtime charges.

7. Custody Receipt

All ECN users who have portable systems equipment must properly complete DL 1-73 Custody Receipt. In accordance with DLMS 2 Chapter 100 - DOL Property Management, a Custody Receipt form is used to record property items issued on long term loan to employees and contractors. Copies of Portable Systems equipment custody receipt forms will be maintained by the ITC.