U.S. Department of Labor

Office of Inspector General
Washington, DC. 20210

June 19, 2012

MEMORANDUM FOR: T. MICHAEL KERR
Chief Information Officer

FROM: ELLIOT P. LEWIS
Assistant Inspector General for Audit

SUBJECT: Alert Memorandum: DOL Needs to Immediately Take Corrective Action to Safeguard BLS Information
Report Number: 23-12-006-07-001

On March 1, 2012, we alerted you to a matter related to the effectiveness of the DOL's electronic media sanitization practices. We identified information technology (IT) equipment that was ready for imminent disposal containing government business information and personal documents. In addition, we identified improper handling of equipment during the sanitization process and inaccurate recording of the equipment in the property management records. (Report No. 23-12-005-07-001, DOL Needs to Immediately Take Corrective Action to Safeguard Information Technology Equipment)

The purpose of this memorandum is to alert you to another matter related to the effectiveness of the Department's electronic media sanitization practices that requires immediate corrective action. We identified Bureau of Labor Statistics (BLS) computers that were ready for imminent disposal containing protected information.

The BLS is responsible for protecting two types of confidential information: respondent identifiable information and pre-release information. Respondent identifiable information is collected from businesses and households by the BLS under a pledge of confidentiality and is protected from unauthorized disclosure and use by the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2002. This information is then aggregated in a manner which allows its release to the public through a statistical report while ensuring respondent identities are not disclosed. Prior to its release to the public, the aggregated statistical report is considered pre-release information. Also, personally identifiable information (PII) must be protected under the requirements of OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information."

On March 22, 2012, the Department signed a memorandum granting approval for the BLS to be responsible for the direct disposal of the BLS IT equipment. It is noted in the memorandum that the BLS will use Departmental forms and meet Departmental requirements, including requirements for the sanitization of IT equipment.

We inspected 60 computers that were ready for imminent disposal, consisting of desktops and laptops, and identified the following major concerns:

- Three hard drives were not sanitized and contained sensitive and statistical information. The hard drives have been identified to belong to two senior economic analysts and one Human Resources staff. Initial analysis of the information contained on these hard drives is provided in the Attachment.

- The hard drives for three computers were missing at the time of OIG testing. BLS had lost accountability over these hard drives and was unable to locate them.

BLS procedures required its Office of Technology and Survey Processing, Division of Network and Information Assurance to perform an audit to mitigate the risk that the IT equipment was not properly sanitized. However, BLS' sanitization verification procedure did not identify the issues noted above.

Based on the results of our limited testing at this point in our audit, it is evident that the BLS is not ensuring sanitization of IT equipment prior to disposal. As a result, the BLS is at risk of unauthorized disclosure of sensitive information, including information covered under the CIPSEA and personally identifiable information. Such unauthorized disclosure could result in BLS staff being subject to criminal fines and penalties for knowingly and willfully mishandling confidential information.

OIG's previous alert recommended that the Department immediately stop disposal of any IT equipment Department-wide until it could ensure that 100 percent of the equipment was being properly sanitized. In response, the Department temporarily stopped all outgoing shipments of IT equipment from the Frances Perkins Building and re-instructed personnel on procedures on movement of IT equipment to ensure accountability of such equipment. However, the results of our testing at the BLS indicate proper sanitization of IT equipment remains a concern not just at the Frances Perkins Building, but at all Department locations.

We recommend that the CIO:

1. Undertake and document a full Department-wide review of all sanitization policies and procedures, including accountability for IT equipment disposals.
2. Immediately stop the BLS from disposing of computers.
3. Rescind the BLS IT Equipment Disposal Authority until the BLS can ensure that 100 percent of the equipment has been properly sanitized.
4. Ensure BLS establishes accountability for all its IT equipment.

5. Instruct BLS to report the 3 missing hard drives to the OCIO as a computer security incident for further investigation.

The results included in this interim report are based on our work to date. Fieldwork is continuing and we will provide overall results when our audit work is complete. Please respond to this report within 3 days with a corrective action plan. Please contact Keith Galayda, Acting Deputy Assistant Inspector General of Audit, at (202) 693-5259, if you have any questions.

Attachment

cc: Edward Hugler
Daniel Lacey

BLS Hard Drives Findings – Unsanitized

Asset Tag: 226295
(Belongs to Senior Economist, Office of Productivity and Technology)

1 BLS statistical documents – spreadsheets and raw data files
2 Hundreds of user's personal pictures
3 User's Citibank Government Travel Card Application Form with PII - name, SSN, DOB, address, email address and phone number
4 User's W-2 form in txt format
5 IP address of computer

Asset Tag: 27064
(Belongs to Program Coordinator, Office of Productivity and Technology)

1 Listing of Foreign Dignitaries Information - Russian Official's Invitation Letter Listing included Russian officials' PII, including names, DOB and position title held in Russian Government
2 IP address of computer

Asset Tag: 225377
(Belongs to Security Assistant, DHROM)

1 File containing 84 individuals' information – identified as PII of employees who were separated from DOL - name, DOB, separation date and SSN.
2 File containing 105 individuals' information – identified as PII of both current and separated DOL employees – name and SSN.
3 EEOC form in txt format - SSN of computer's user
4 IP address of computer