SEP 22 2000

MEMORANDUM FOR: KATHARINE G. ABRAHAM
Commissioner, Bureau of
Labor Statistics

/ S /

FROM: JOHN J. GETEK
Assistant Inspector General
for Audit

SUBJECT: BLS Data Security Followup Audit
Final Letter Report No. 03-00-012-11-001

This final letter report provides the results of our followup audit to the Office of Inspector General (OIG) report entitled *BLS Information Technology, Survey Processing, and Administrative Controls Must be Improved*, Audit Report Number 09-99-007-11-001, issued July 20, 1999.

The letter report contains details on the audit results of the four recommendations that were open during our fieldwork and a finding and recommendation on a weakness in UNIX server passwords that was unrelated to the previous report recommendations. As a result of your response to the draft letter report, two of the four previous report recommendations were closed and the recommendation concerning the weakness in the UNIX server passwords was resolved.

Please keep us informed of your actions to close the three remaining recommendations.

We thank Stuart Rust and his staff for their courtesy and cooperation extended to the auditors during the fieldwork.

If you have any questions concerning this report, please contact Roger B. Langsdale, Regional Inspector General for Audit, in Philadelphia at (215) 656-2300.

Background, Objectives, and Scope

On July 20, 1999, OIG issued an audit report to the Bureau of Labor Statistics (BLS) entitled *BLS Information Technology, Survey Processing, and Administrative Controls Must be Improved*. The audit was initiated as a result of a BLS prerelease of employment data in November 1998. The purpose of the audit was to determine whether adequate and effective internal controls were in place to prevent the premature or unauthorized disclosure or use of sensitive economic data. The audit scope was limited to five mission-critical systems involved in producing and disseminating reports that could have the most impact on financial markets if released before schedule: Current Employment Statistics Survey, Current Population Survey, Consumer Price Index, Employment Cost Index, and Producer Price Index. BLS Regional Offices were not included in the audit. The audit report contained 41 recommendations.

We performed a followup audit to determine if BLS implemented the recommendations in the July 20, 1999, audit report. The followup audit covered BLS National Office operations as they existed at the time of our field work, June 5 through August 21, 2000, and considered any planned future changes. To accomplish our audit, we reviewed written policies and procedures and identified controls related to the findings from the prior audit report. We also made observations and performed tests to determine if BLS policies, procedures, and internal controls were in place, effective, and adhered to. In addition, we performed access control tests to determine if password strength was adequate.

The audit was performed in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

Audit Results

The results of our fieldwork found that BLS had sufficiently implemented 37 of the 41 recommendations. On August 25, 2000, we sent the BLS Commissioner a draft letter report for her comments. The Commissioner's response, attached in its entirety, resulted in closing two more recommendations. BLS should be commended for the resources and effort put forth to implement the recommendations.

Also, during the audit we found a weakness in a user password on a UNIX server. The corrective action needed to improve UNIX user passwords did not apply to any recommendations in the previous report. Therefore, the draft letter report contained an additional finding and recommendation. The recommendation was resolved as a result of the Commissioner's response.

Details of the audit results follow.

Recommendation No. 1.2.1: Ensure procedures are developed to periodically review and test

access controls at SunGard Computer Services to ensure BLS data is secure.

This recommendation was open because BLS had not fully implemented its procedures to test file and tape access controls at SunGard Computer Services (SunGard). We also found that access control deficiencies still existed at SunGard.

BLS developed test procedures to verify that BLS information stored on tapes at SunGard is secure. The test procedures entail setting up an "outside account" (an account not related to BLS) with SunGard, and using the account to process tape cartridge access programs against BLS tape cartridges to determine if they can be accessed. The procedures require that the tests be performed twice a year. We concluded that the planned procedures would be effective once implemented. However, at the time of our field work, the test procedures had not been implemented because SunGard has been reluctant to provide the needed outside account.

We tested SunGard access controls and found deficiencies still exist. An OIG computer specialist was able to access, read, and copy data from a BLS tape. To determine if the problem could impact other DOL agencies, we arranged for a BLS computer specialist to attempt to access and read an OIG tape. The attempt was successful. We consider these penetrations to be a serious breach of security that may place all DOL tapes in jeopardy of unauthorized access. Although both computer specialists needed a tape number to perform the tests, an unauthorized user could easily obtain this information from printouts that are routinely thrown into recycling or trash containers.

BLS has discussed this matter with SunGard officials, and we informed the DOL Chief Information Officer about the access control problems at SunGard. Since this incident, BLS has made an agreement with the DOL Office of Chief Financial Officer (OCFO) to establish SunGard accounts for security testing.

Action Needed to Close the Recommendation

BLS must finalize its agreement with the OCFO and establish the outside account for security testing at SunGard.

BLS Response

BLS finalized its agreement with the OCFO to exchange SunGard user accounts.

OIG Conclusion

This recommendation is closed.

Recommendation No. 1.4.4: Develop and implement Information Technology (IT) security procedures to require that all servers and backup media be located in a secure location with limited access.

This recommendation remains open because BLS has not decided which options presented in the "Server Consolidation Options Report" will be the most cost effective approach for ensuring that all servers and backup media are located in a secure location with limited access.

The BLS Office of Technology and Survey Processing (OTSP) chartered a team to review the physical location and logical administration of all servers within BLS. In May 2000, the OTSP team issued the "Server Consolidation Options Report," which presented four options for consolidating servers. However, BLS officials told us they are doing further research on some options before making a final decision. They expect this to occur in the next 2 to 3 months.

We reviewed the physical security of servers in the five survey offices cited in the audit. We found that the same condition reported in the audit continues to exist except that servers used to store embargoed data have been secured.

Corrective Action Needed to Close the Recommendation

BLS must provide a plan that will ensure that all servers and backup media are located in a secure location with limited access.

BLS Response

BLS will inform us when they determine their course of action regarding server location and administration.

OIG Conclusion

This recommendation remains open.

Recommendation No. 1.4.7: Identify and review all existing data lines to ensure that they are needed.

This recommendation was open because we found that two modems allowing dial-in access were not secure. Although BLS does review its data lines to ensure they are needed, this procedure did not identify modems that are not properly configured or protected.

As part of our audit, we conducted a phone sweep to detect modems within the BLS National Office. We identified two modems connected to BLS computers that were configured to receive incoming calls. We were told that one modem is used to connect to SunGard. In this case, the modem should be configured to perform outgoing calls only. The other modem has a valid reason for allowing dial-in access. However, a subsequent access test we performed revealed that access through this modem did not require a username and password.

Modems that are not properly configured and protected are security risks because they provide additional points of entry into the BLS network and bypass central protective devices such as a firewall.

Action Needed to Close the Recommendation

BLS must perform regular tests to ensure that modems not requiring dial-in access are configured for outgoing calls only. Computers that require dial-in access should be protected by a username and password, and should display the BLS security warning banner during log-on.

BLS Response

BLS changed the modem line to SunGard to permit dial-out calls only. The other modem identified in the report now prompts for an appropriate user name and password. BLS also responded that phone sweeps will be performed quarterly to detect unauthorized modems. Additionally, every BLS computer providing dial-in access will be protected by a username and password and, where possible, the BLS security warning banner will be displayed during the log-on process.

OIG Conclusion

This recommendation is closed.

Recommendation No. 1.4.8: Ensure managers review computer accounts regularly and verify that each account should be kept active. Delete all inactive accounts and accounts of separated employees and contractors.

This recommendation remains open. Although we found no exceptions in our review of NT servers, we did find that separated BLS employees still had active user accounts on UNIX servers. Because UNIX servers are not centralized, the process for reviewing and verifying user accounts is more difficult than for NT servers.

BLS implemented a review process which covers the deletion of user accounts for separated BLS employees, deletion of inactive user accounts not used within the last 30 days (after confirming an account is not needed), and an annual review of user accounts by network administrators.

To determine if the review process was working, we obtained a list of employees who separated from BLS during the period January 2 through June 19, 2000, and compared it to active NT and UNIX user accounts. We were told that the UNIX servers are not centralized and each individual server has its own accounts and passwords. Because of time restraints, we did not request a complete list of active UNIX accounts. Instead, BLS provided to us a list of active user accounts for approximately 75 percent of the UNIX servers using special software to compile user data.

We found no exceptions in our comparison of separated BLS employees to active NT user accounts. However, we found two separated employees still had active UNIX user accounts.

BLS is currently creating a "meta-directory" that will enable them to access centralized user data from all of their UNIX servers.

Action Needed to Close the Recommendation

BLS must complete the "meta-directory" and begin testing their UNIX servers to ensure that user accounts for separated employees are deleted.

BLS Response

BLS will inform us when the 'meta-directory' is completed and central monitoring of UNIX accounts is under way.

OIG Conclusion

This recommendation remains open.

User Password Strength Needs to be Improved

We performed additional access control tests to check the strength of user passwords on a Windows NT server and a UNIX server. To accomplish this, we used password auditing software to examine approximately 180 user passwords on the NT server and 100 user passwords on the UNIX server. No exceptions were found on the NT server; however, we were able to crack one password immediately on the UNIX server because the password was identical to the username. We were told that the employee no longer worked for BLS and an administrator had set up the account but it was never used. The account should have been deleted.

The BLS Security Officer told us that because user account data is not centralized within the UNIX environment, it is difficult to run this type of test on each individual server. However, BLS is considering using a program that will allow them to test user password strength from all their UNIX servers, and they could run a centralized test with this.

Recommendation

We recommend that BLS implement a program to periodically use password auditing software to test the strength of UNIX user passwords.

BLS Response

BLS responded that they will begin testing user password strength on all UNIX accounts in the near future.

OIG Recommendation

This recommendation is resolved; but remains open.

Attachment