Office of Inspector General

U.S. Department of Labor
Office of Audit

BLS Information Technology, Survey Processing and Administrative Controls Must be Improved

Report Number: 09-99-007-11-001
Date Issued: July 20, 1999

TABLE OF CONTENTS

ACRONYMS

ADP	Automatic Data Processing
BI	Background Investigation
BLS	Bureau of Labor Statistics
CES	Current Employment Statistics (Establishment)
COOP	Continuity of Operations Plans
CPI	Consumer Price Index
CPS	Current Population (Household) Survey
DOL	Department of Labor
DPPS	Division of Producer Price Systems
DSM	Division of Systems Modernization
ECI	Employment Cost Index
ETA	Employment and Training Administration
ESR	Employment Situation Report
FIPS	Federal Information Processing Standards
FSMS	Federal State Monthly Surveys
GAO	General Accounting Office
GSA	General Services Administration
IT	Information Technology
LABSTAT	Labor Statistics
LAN	Local Area Network
LBI	Limited Background Investigation
MBI	Minimum Background Investigation
NACI	National Agency Check and Inquiries
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NT	New Technology
OA	Office of Administration
OGE	Office of Government Ethics
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPLC	Office of Prices and Living Conditions
OPSS	Office of Publications and Special Studies
OPM	Office of Personnel Management
OTSP	Office of Technology and Survey Processing
PC	Personal Computer
PPI	Producer Price Index
PSB	Postal Square Building
RACF	Resource Access Control Facility
TRP	Triennial Review Plan

EXECUTIVE SUMMARY

Subsequent to a prerelease of employment data which occurred on November 4, 1998, the Bureau of Labor Statistics (BLS) Commissioner requested the Office of Inspector General (OIG) to perform a comprehensive audit of activities associated with the dissemination of sensitive BLS data. Early in OIG's field work, another prerelease occurred. The December Producer Price Index was released a day early on January 12, 1999. Another incident occurred on January 22, 1999, when an intruder altered a BLS web page.

Our audit findings demonstrate that, over a period of time, the BLS operated its Information Technology (IT) security, survey processing and certain administrative procedures without the benefit of sound internal controls. In our opinion, this absence of a strong control environment contributed to the premature release of sensitive BLS data.

This report is divided into three chapters. The **first** chapter addresses IT security vulnerabilities. The **second** chapter focuses on inconsistencies in security practices in program survey offices. Chapter **three** deals with administrative deficiencies in personnel security and management oversight. Each chapter includes the findings related to the subject area and BLS' response to our Statement of Facts and draft report. OIG's recommendations for corrective action are included in each chapter. BLS has expeditiously acted (or started action) on most of our recommendations.

Within each chapter, there are numerous audit findings. When considered separately, an individual finding might be construed as having a "minor" impact on BLS security over sensitive economic data. However, when taken as a whole, these findings show pervasive problems in the BLS internal control structure.

Information Technology Security Vulnerabilities

The Office of Technology and Survey Processing (OTSP) is responsible for BLS IT. We focused our audit efforts on identifying and evaluating IT internal controls developed and implemented by OTSP. We identified internal control deficiencies in four areas we believe are critical in successfully managing an IT department:

! control deficiencies existed in web site operations;

! access control deficiencies existed in tape cartridge security at SunGard Computer Services;

! management controls over survey application software testing and protection were inadequate; and

! security vulnerabilities existed in the local area network (LAN) infrastructure.

These vulnerabilities threaten the integrity of sensitive BLS data. BLS internal controls over systems and applications software were inadequate and contributed to one of the prerelease incidents. Other vulnerabilities existed in the operations of the BLS LAN systems and web site.

Inconsistent Security Practices in Program Survey Offices

There were inconsistencies among program survey offices regarding the level of security over news release preparation. The policies and procedures varied for news release preparation and the documentation of the procedures was fragmented and incomplete. Documents and electronic files with sensitive and confidential data were not always afforded appropriate levels of protection. Policies and procedures for staff working on flexiplace did not specifically address security issues.

Deficient Personnel Security and Management Control

We found numerous deficiencies in the area of personnel security. The sensitivity classification of most of the positions we reviewed was inaccurate, indicating most were nonsensitive when in fact the individual occupying the position handled sensitive information. This, combined with the fact that many staff handling sensitive information had no security clearance pointed to a lack of control over this critical area. Periodic training and reminders of ethics responsibilities and investment restrictions were not provided to all staff who handle sensitive information.

Management controls did not appear effective due to the lack of regular reviews and audits of BLS operations and security practices. There was also a lack of effective follow-up to ensure issues identified in previous studies were corrected.

Weaknesses in oversight, absence of written policies and procedures over computer systems and preparation of the news releases, and the absence of security practices, led to security incidents and placed the agency's sensitive and confidential data at risk.

Conclusion

BLS data have become increasingly difficult to protect due to advances over the past few years in easy-to-use, high-level-inquiry languages, the spread of ever more powerful small computers, the accelerating use of the Internet, and general increases in computer literacy. All of these developments have created a higher level of risk and, consequently, protection requirements for IT systems.

Without a corresponding growth in good data security practices and internal controls, these advances increase the risk of inadvertent or deliberate corruption of BLS data assets.

BLS has recently initiated numerous reviews, and formed several committees since the security incidents. However, similar studies in the past have come and gone without effective follow-up to assure the implementation of the recommended changes. This time, there must be the highest level of oversight to ensure effective follow-through on all identified issues. To do otherwise would increase the possibility of future security incidents.

We believe it is imperative the Bureau act promptly to correct the deficiencies both we and they have identified. Further errors in the timing of news releases or other security breaches may compromise BLS' reputation and credibility, as well as erode public confidence in BLS reports.

BLS Response to Draft Report

BLS said it was in general agreement with the findings and recommendations, which have already been quite helpful in improving the security of BLS programs. Corrective action is under way and several of the recommendations have been fully implemented. Projected completion dates have been provided where work still is under way. The full text of BLS' response is included as Exhibit I of this report.

OIG Conclusion

Actions BLS is taking, or proposes to take, generally satisfy OIG recommendations. However, we note BLS' timetable shows that some actions will not be completed until future dates, extending to the year 2002. In some instances, BLS does not fully agree with OIG's recommendation and is proposing alternative actions. We urge BLS to expedite its corrective actions wherever possible and fully implement OIG recommendations. OIG's specific conclusion to BLS' response to each recommendation is included in the text of this report. The OIG plans to conduct a follow-up audit on BLS' corrective actions taken to resolve this audit report.

OBJECTIVES, SCOPE, METHODOLOGY AND CRITERIA

Objectives

The overall audit objective was to determine if the Bureau of Labor Statistics (BLS) had adequate and effective internal controls in place to prevent the premature or unauthorized disclosure or use of the following sensitive economic data:

- employment trend indicators;
- indicators of inflationary trends; and
- economic information used by the Federal Reserve Board in setting monetary policy.

Our specific audit objectives were to identify data and reports BLS considered to be sensitive and embargoed (time sensitive, i.e., must not be released before a set date and time) and determine:

- whether internal control policies, procedures and structure provide reasonable protection of agency information assets;
- the levels of review (control) for all work performed on relevant systems, data collection, analysis/conversion of data into sensitive information; and
- if employees and contractors with access to systems, data and information are properly screened, trained and subject to financial disclosure reporting requirements.

Scope

Our audit covered BLS national office operations as they existed at the time of our field work (January 5 through April 9, 1999) and addressed BLS planned initiatives. BLS advised us they operated 23 mission-critical systems. We performed audit field work in BLS national office organizations and systems involved in producing and disseminating the sensitive reports that can have the most impact on financial markets if released before scheduled. These reports are produced by the following five mission-critical systems (surveys):

- Current Employment Statistics (Establishment) Survey (CES);

- Current Population (Household) Survey (CPS);

- Consumer Price Index (CPI);

- Employment Cost Index (ECI); and

- Producer Price Index (PPI).

The CES and CPS survey information are combined and published as the Employment Situation Report (ESR). We excluded BLS Regional Offices from our audit. We did not audit data collection and editing operations at the U.S. Bureau of the Census in its role of providing BLS Current Population (Household) Survey information.

As discussed in Chapter I, at the time of our review the National Security Agency (NSA) initiated a security review of the BLS web site. The review included installing sophisticated security-testing software on the web server to detect potential vulnerabilities. We did not perform procedures that would duplicate NSA work.

Methodology

To accomplish our audit, we reviewed written policies and procedures and identified the controls over collecting, analyzing, processing and reporting sensitive data. We conducted interviews with BLS officials and staff, walked through survey press release preparation activities and made observations to determine if BLS policies, procedures and internal control structures were in place, operational and adhered to. The nature of this audit did not require the use of statistical sampling.

We discussed our observations and findings with BLS officials and staff during the course of field work. We provided BLS officials interim status reports. At the conclusion of field work, we issued a Statement of Facts (with summary workpapers as attachments) to the Commissioner. BLS provided us a comprehensive written response to the Statement of Facts.

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

Criteria

The following criteria were used in accomplishing our audit:

- C OMB Circular No. A-123 - Management Accountability and Control, June 1995
- C OMB Circular No. A-130 - Management of Federal Information Resources, February 1996
- C BLS Information Technology Security Manual, Version 1.3, dated November 4, 1998
- C NIST Special Publication 800-12 - An Introduction to Computer Security dated October 1995
- C NIST Special Pub. 800-18 - Guide for Developing Security Plan for IT Systems
- C FIPS Pub 191 - Guideline for the Analysis of Local Area Network Security
- C FIPS Pub 112 - Password Usage
- C GAO/AIMD-98-12.19.6 - GAO Federal Information System Controls Audit Manual, January 1999
- C GAO/AIMD-98-21.3.1 - GAO Standards for Internal Control in the Federal Government, December 1997
- C Federal Personnel Manual
- C Security Plan for the Employment Situation Current Population Survey (CPS) System, November 1998
- C Producer Price Index (PPI) System Security Plan, November 1998
- C CPI Data Security Procedures, June 1998
- C Standards of Ethical Conduct for Employees of the Executive Branch, August 1992
- C BLS Personal Data Security Practices
- C Administrative Procedure 1-96, Responsibility for Safeguarding Confidential Information
- C Commissioner’s Order 3-93, Confidential Nature of BLS Records
- C Commissioner’s Order 1-96, Consumer Price Index Futures Contracts

BACKGROUND

On Wednesday, November 4, 1998, a prerelease of Bureau of Labor Statistics' (BLS) employment data for the month of October 1998 occurred. This data release should not have occurred until Friday, November 6, 1998. The early release affected both stock and bond market prices. The BLS Commissioner requested the Office of Inspector General (OIG) perform a comprehensive audit of activities associated with the dissemination of sensitive BLS data.

The BLS Commissioner also directed an internal review be immediately initiated. An internal report on the review was issued on November 19, 1998. The BLS report concluded the prerelease was accidental and resulted from inadequate management and internal controls over the handling of supplemental information. The report also concluded that the rigorous, centralized procedures which govern the posting of news releases and time series data on the web site were not uniformly applied to the handling of supplementary materials.

BLS Organization Background

BLS is the principal data-gathering agency of the Federal Government in the broad field of labor economics and statistics. BLS is a national statistical agency that collects, processes, analyzes and publishes sensitive statistical and economic data in areas identified for economic research and statistical fact-finding by Congress, other Federal agencies, state governments, business and labor.

Most of the Bureau's data come from voluntary responses to business and household surveys conducted by BLS staff, the Bureau of the Census (on a contract basis), and in conjunction with cooperating state and Federal agencies. Voluntary reporting from businesses and households and the preserving of the confidential nature of reported data are important characteristics of BLS programs.

All BLS programs meet statutory responsibilities. The legislation establishing BLS in the late 1800s (29 U.S.C. l) states:

> *The general design and duties of the Bureau of Labor [Statistics] shall be to acquire and diffuse among the people of the United States useful information on subjects connected with labor, in the most general and comprehensive sense of that word, and especially upon its relation to capital, the hours of labor, the earning of laboring men and women, and the means of promoting their material, social, intellectual, and moral prosperity.*

BLS data and statistical survey results are used in the development of other Federal statistics, including the Gross Domestic Product, and economic indicators. Congress, the President, the Federal Reserve Board, and other executive branch agencies rely on these indicators and BLS data to determine national economic policy. BLS data and survey results are also used by industry and labor in economic planning and collective bargaining activities and by other public and private institutions for a variety of planning and analytical activities.

BLS developed the statistical survey programs, for the most part, independently from each other. As a result, the Bureau was organized according to survey subject matter areas, an arrangement which has been continued over the years. Each subject matter group, or survey, has an information technology support group within the Office of Technology and Survey Processing.

INTRODUCTION

This report is divided into three chapters. The first chapter addresses information technology (IT) security vulnerabilities. The second chapter focuses on inconsistencies in security practices in program survey offices. The third chapter deals with administrative deficiencies in personnel security and management oversight. Each chapter includes the findings related to the subject area and BLS' response to our Statement of Facts. OIG's recommendations for corrective action are included in each chapter. BLS has expeditiously acted (or started action) on most of the OIG recommendations.

Within each chapter, there are numerous audit findings. When considered separately, an individual finding might be construed as having a "minor" impact on BLS security over sensitive economic data. However, our findings demonstrate pervasive problems exist in BLS' approach to IT security. In our opinion, the extent of our findings is indicative of an agency that has, over a period of time, had a breakdown in administering and enforcing IT security.

Some of the issues identified in this audit report were identified in previous reviews by various entities. BLS did not act effectively to correct the problems identified. BLS internal reviews conducted as a result of the two prereleases of data identified many of the same IT security issues previously identified.

In our opinion, weaknesses in oversight, absence of written policies and procedures over computer systems and preparation of the news releases, and the absence of security practices, led to security incidents and placed the agency's sensitive and confidential data at risk.

FINDINGS AND RECOMMENDATIONS

Chapter I Information Technology Security Vulnerabilities

OTSP is responsible for BLS IT. OTSP provides technical support to the BLS program surveys. OTSP's Labor Statistics (LABSTAT) group is responsible for posting news releases and related data to the BLS public web site.

We focused our audit efforts on identifying and evaluating IT internal control structures developed and implemented within OTSP. We identified the following deficiencies:

1. control deficiencies existed in web site operations;
2. access control deficiencies existed in tape cartridge security at SunGard Computer Services;
3. management controls over survey application software testing and protection were inadequate; and
4. Security vulnerabilities existed in the local area network infrastructure.

We believe these deficiencies are significant. They indicate a pervasive lack of management control and oversight in this critical area. BLS must move quickly to rectify these problems to avoid further disclosures and ensure sensitive data are not compromised.

1. Control Deficiencies Existed in Web Site Operations

Inadequate internal control structures in LABSTAT led to prereleases and the web site intrusion incident. LABSTAT management did not recognize the commitment needed to implement effective internal controls as the web site and the Internet grew more complex. The Bureau's efforts to meet increasing public demand for timely access to data releases appear to have outweighed LABSTAT efforts to ensure adequate controls were implemented. BLS did not institute procedures to ensure risks were identified and fully understood.

As a result, problems have occurred in the release of data to the BLS web site. There have been three incidents of premature releases of embargoed BLS data in the past 3 years. Continuation of these problems could erode public confidence in BLS' ability to properly disseminate economic information at prescribed times.

In response to the prereleases, the Commissioner directed LABSTAT management to implement interim procedures that do not allow the news releases and related data to be transferred to the web site server until shortly before or at release time.

LABSTAT is responsible for posting sensitive economic data such as job growth, unemployment rates and price changes to the BLS web site. LABSTAT is also responsible for the operation and maintenance of the web site. The economic information on the BLS web site is extremely valuable and used by many governmental and private organizations in making key financial and policy decisions. Individuals with advance knowledge of BLS information could exploit the information for their own financial advantage.

The Employment Situation Report (ESR), Producer Price Index (PPI), and Consumer Price Index (CPI) are posted monthly to the web site. The Employment Cost Index (ECI) is posted quarterly. Program offices analyze survey data and prepare reports and indexes. The program offices submit the results of their analysis to LABSTAT for processing and posting to the BLS web site.

LABSTAT's critical role in processing and disseminating sensitive economic information mandates strong, effective internal controls be in place and operational to ensure data is properly safeguarded and released at the appropriate time. However, we determined management controls for safeguarding and posting data to the BLS web site were not effective. Ineffective controls contributed to both the inadvertent prereleases of economic reports and the intrusion and hacking of the web site.

Our audit work disclosed the following problems:

a. web site servers were vulnerable to intrusion;

b. application software development and change control procedures were inadequate;

c. system software and application programs were being tested simultaneously in the same environment;

d. timely training was not provided to staff when new processes were implemented;

e. LABSTAT lacked formal lines of communications and definition of responsibilities; and

f. program staff outside LABSTAT posted information to the web site.

a. Web Site Servers Were Vulnerable to Intrusion

On January 22, 1999, an unknown individual hacked into the BLS public web site. The hacker put an obscene message on the BLS home page. BLS determined the hacker gained access through a software product called Microsoft FrontPage. BLS had installed the product according to defaults and had not enabled all security features. This oversight allowed the hacker to deface the web page.

On February 9, 1999, the National Security Agency (NSA) initiated a security review of the BLS web site. NSA installed sophisticated security-testing software on the web servers to detect potential vulnerabilities. NSA has not issued its final report. However, preliminary indications are NSA identified high-risk vulnerabilities impacting system integrity. The “raw data” produced by one of the vulnerability analysis software packages contains the following warning:

> *. . . It is highly probable that a remote attacker can gain complete control over these systems, and use them to leverage access to other resources on the network.*

We did not attempt to duplicate or extend the NSA tests; rather, their tests and analysis are incorporated into this report by reference. In our opinion, NSA security-testing software is sufficiently creditable to conclude there are vulnerabilities in the web servers. BLS has taken actions to reduce some of the NSA-identified vulnerabilities and will act on others, as appropriate, when the final report is delivered.

At our May 21, 1999 exit conference, BLS provided us a copy of NSA’s final report, dated May 13, 1999. The report identified many high risk vulnerabilities that BLS needs to address immediately and contained recommendations for corrective action.

b. Application Software Development and Change Control Procedures Were Inadequate

On January 12, 1999 (after audit field work commenced), BLS inadvertently released PPI data early. The premature release would not have occurred if adequate internal controls had been in place and enforced. Internal control deficiencies discussed below contributed to this error.

(1) LABSTAT did not have formal written procedures for requesting and approving program changes. There was no requirement to document each change, test results, and to have supervisory review and approval. Procedures were not formalized for migrating tested programs (after an independent review) into the production library.

(2) LABSTAT development staff routinely copied programs (referred to as scripts) from the production computer to the test computer for modification and testing. The same programmer then migrated the "tested" program back to the production computer. We found program changes were not being independently tested; i.e., tested by an independent review/quality assurance group.

(3) LABSTAT was not using standard automated tracking software to control software libraries. Consequently, (a) an unauthorized program could be substituted for the authorized version; (b) test programs could be labeled as production programs; (c) two programmers could inadvertently access and work on the same test program version simultaneously, making it difficult or impossible to merge their work; and (d) unauthorized changes to either test or production programs could be made surreptitiously and remain undetected.

The BLS response to our Statement of Facts indicated LABSTAT is currently implementing more stringent controls over software changes and testing. Additional staff is being hired to perform these processes. A team was recently commissioned to make recommendations on configuration management. LABSTAT will hire a librarian to control access to production systems. File permissions for production scripts have been set so that modifications can be made only by the production team leader. LABSTAT installed Visual Source Safe version control software the week of March 22, 1999.

c. System Software and Application Programs Were Being Tested Simultaneously in the Same Environment

LABSTAT did not have adequate policies and procedures to control system software and application program testing. Development staff tested new versions of system software on the development server while also testing updated application programs on the same server.

The January 1999 PPI prerelease was caused, in part, by the simultaneous testing of system software and application programs on the same server. The System Administrator was supposed to maintain identical versions of system software on both the development and production servers. However, a programmer obtained a more current shareware version of some software and loaded it on the development server. He then made modifications to a date field in an application program and tested the change on the development server. The application program test ran successfully on the development server. The programmer migrated the changed application program to the production server which was running an older version of the system software. The application program subsequently failed, resulting in the prerelease of the PPI news release data.

BLS responded to our Statement of Facts as follows:

> *LABSTAT has implemented changes to adhere fully to existing BLS system software standards, policies, and procedures. In addition, LABSTAT is developing a project-specific policy manual with supplemental materials. The first draft of this manual was issued to staff and discussed in detail on April 7, 1999.*

d. Timely Training Was Not Provided to Staff When New Processes Were Implemented

LABSTAT personnel were not trained when processes were changed. This lack of training in new processes contributed, in part, to the January 1999 prerelease of the PPI.

Regarding the January 1999 PPI prerelease, we determined the LABSTAT computer operator recognized the PPI press report would be released a day early. He changed the scheduled release date in the computer and went to lunch. Under the old procedures, changing the scheduled release date in the computer would change the date the job would run. Unknown to the computer operator, new automated procedures were in effect and changing the date on the computer would not prevent the job from running. When the computer operator returned from lunch, he found the PPI job ran and the press release was in the public domain.

BLS responded to our Statement of Facts as follows:

> *The BLS agrees with the OIG that a lack of training in new procedures in the LABSTAT Branch contributed to the January prerelease incident. The LABSTAT Branch has instituted a process whereby staff are trained on all new procedures during the testing phase.*

e. LABSTAT Lacked Formal Lines of Communications and Definition of Responsibilities

LABSTAT lacked effective formal lines of communication between staff and management. Effective communication is an essential requirement in managing an IT department. Formal lines of communication ensure management is kept abreast of problems that can arise daily.

Preceding the January 1999 PPI prerelease, a LABSTAT programmer told the computer operator he had identified a problem in an application program used to post the news release to the web site. The computer operator thought the programmer meant that he had corrected the problem. The programmer then went to lunch, intending to fix and test the script when he returned. In the meantime, the PPI program supervisor, not knowing of the programming problem, followed normal procedures and electronically approved the press release for posting the next morning. The program failed and the job ran almost immediately, prematurely posting the PPI news release to the web site. Both the computer operator and the programmer knew there was a programming problem. However, neither had reported this information to either their supervisor or the PPI program supervisor.

OIG and BLS jointly interviewed LABSTAT personnel regarding this prerelease. In its report BLS concluded: (1) LABSTAT branch development, testing, and installation of programs are not tightly controlled, coordinated, and recorded in accordance with accepted systems development methods, and (2) procedures for these activities and areas of responsibility are informal and not documented. No one person has official responsibility for coordinating revisions to programs.

BLS responded to our Statement of Facts as follows:

> *The LABSTAT Branch has prepared a detailed organization chart and overview of staffing duties and responsibilities as required for a planned reorganization of the unit. These documents have been reviewed and approved by OTSP and OA management. . . LABSTAT Branch is filling the currently vacant Branch Chief position, an action which should improve the situation regarding formal lines of communication.*

f. Program Staff Outside LABSTAT Posted Information to the Web Site

On November 4, 1998, BLS prereleased nonfarm payroll employment survey information to the public web site. The data was scheduled to be released two days later on November 6, 1998, as a supplement to the Employment Situation News Release. An economist employed in a program office outside of LABSTAT was given the responsibility of posting this data to the web site. The BLS security review of this incident stated the premature release of data to the web site was a result of miscommunication between a senior economist and an economist who were given the task to post the data to the web site. The BLS conclusion, in part, may be correct; however, BLS needs to establish clear responsibilities for posting embargoed data to the public web site. In our opinion, in the absence of this designated responsibility, BLS remains vulnerable to prereleases of embargoed information.

Further, we believe relying on an economist outside of LABSTAT, with limited training and inadequate documentation and procedures to post data to the BLS web site, was inappropriate.

Recommendations

To properly safeguard economic information, provide for the timely release of accurate data at prescribed times, and maintain public confidence in BLS dissemination of data on its web site, we recommend the Commissioner take the following actions:

1. Establish controls to ensure all available web security features are enabled.

2. Act on all findings in the NSA Security Report.

3. Require LABSTAT to obtain and implement a standard library management system to protect software.

4. Develop policies and procedures for LABSTAT which provide for controls over changes, upgrades, testing and implementation of both system and application software.

5. Require the independent review/quality assurance function be performed for all modifications before placing programs or systems into production.

6. Restrict access to all programming source code.

7. Ensure LABSTAT develops formal documentation outlining duties, responsibilities and lines of communication.

8. Ensure staff outside of LABSTAT is not allowed to post information to the web site.

BLS Response to the Draft Report

BLS' response is summarized below and numbered to correspond with OIG's recommendations. The complete text of BLS' response is contained in Exhibit I of this report.

1. New web software (Microsoft Internet Information Server 4.0) has been installed and comprehensively configured. Security scripts were run to test for the presence of recommended patches. Security-related news services are being monitored to keep abreast of threats and appropriate countermeasures.

2. BLS has made changes to implement 37 of NSA's 82 recommendations. Some of the recommendations may not be implemented without making some of the BLS web site unavailable to the public. BLS is evaluating the NSA's recommendations and will review the results with OIG. Implementation should be completed, to the extent possible, by November 1999.

3. LABSTAT has implemented Microsoft Visual Source Safe version control software. Data loading scripts have been entered. Other LABSTAT source code is currently being entered. Implementation should be completed by August 1999.

4. Implementation is under way and should be completed by January 2000. General policies have been set. Version control software is in place. Specific procedures will be developed and implemented when a staff member is hired to be a librarian and configuration management coordinator.

5. Implementation is under way and should be completed by November 1999. LABSTAT established a new independent Quality Control team in February 1999. Comprehensive test plans have been developed and two rounds of independent testing have been performed.

6. Access to LABSTAT programming source code has been restricted so that only the Data Management branch chief has write access to data loading scripts on the production machines.

7. Implementation is under way and should be completed by January 2000. LABSTAT is working on a comprehensive reorganization plan.

8. File permissions on LABSTAT production machines have been set so that only LABSTAT staff may write to the machines.

OIG Conclusion

Based on BLS' response to our Statement of Facts and draft audit report, OIG considers the above recommendations to be resolved. The recommendations can be closed when BLS provides adequate documentation that the corrective action has been implemented.

2. Access Control Deficiencies Existed in Tape Cartridge Security at SunGard Computer Services

BLS tape cartridges (and all other DOL tape cartridges) at a mainframe computer contracted by DOL were vulnerable to unauthorized access.

In addition to the computer servers BLS operates, it also purchases mainframe computer support from SunGard Computer Services. Much of the survey micro data BLS collects is transmitted to SunGard where it is edited, analyzed, summarized, and then returned to the BLS servers. Other Department of Labor (DOL) agencies, including OIG, use the SunGard service facility. Data at SunGard are typically stored on magnetic media such as disks and tape cartridges. SunGard's security software, Resource Access Control Facility (RACF), was supposed to protect data files from unauthorized access.

Our audit work disclosed BLS tape cartridges (and all other DOL tape cartridges) at SunGard were vulnerable to unauthorized access. We were able to penetrate the tape cartridge security system at SunGard. An OIG computer specialist at a remote location obtained access to BLS tape cartridge files stored on SunGard.

BLS responded that the tape cartridge vulnerability was a SunGard deficiency affecting all DOL SunGard users. (OIG notified the DOL Chief Information Officer of this vulnerability.) OIG has retested the tape cartridge security and found the vulnerability has been eliminated.

BLS believes the tape cartridge [unauthorized] access problem was a SunGard problem which affected all DOL SunGard users. Regardless, BLS (and other DOL agencies are) is responsible for protecting its IT assets. Consequently, we believe it is incumbent on the using agency to test the security systems provided by external computer services.

Recommendation

To improve security of data at SunGard, we recommend the Commissioner ensure procedures are developed to periodically review and test access controls at SunGard to ensure BLS data is secure.

BLS Response to the Draft Report

BLS responded that implementation of the recommendation is under way and should be completed by October 1999. The BLS Information Technology (IT) Security Team has been assigned the responsibility for testing IT security controls at SunGard. They will develop/acquire tools and establish procedures for regularly testing file and tape access controls at SunGard.

OIG Conclusion

Based on BLS' response to our Statement of Facts and draft audit report, OIG considers the above recommendation to be resolved. The recommendation can be closed when BLS provides adequate documentation that the corrective action has been implemented.

3. Management Controls Over Survey Application Software Testing and Protection Were Inadequate

BLS has organized the IT function largely by survey. Separate OTSP units provide IT support for each program survey. The program survey funds the OTSP unit serving it. Periodic economic reports produced by the surveys are transmitted to LABSTAT for posting to the BLS web site.

BLS relies heavily on IT to carry out its mission of providing statistics to the public and other government agencies. Each survey has its own sophisticated software systems developed over years. These software systems represent an enormous investment in time and money. The protection of these IT assets is critical.

This decentralization led to internal control inconsistences within the surveys. Our audit of program survey office IT operations disclosed the following deficiencies:

a. some surveys were not using independent review/quality assurance groups to test software;

b. access to programming source code was not restricted on the mainframe computer; and

c. some surveys were not using a standard library management system to protect software.

a. Some Surveys Were Not Using Independent Review/Quality Assurance Groups to Test Software

During our audit, we found some surveys performed final testing of application software modifications without using an independent review/quality assurance group. As a result, there was no assurance that modified computer programs operated as intended and unauthorized changes were not introduced.

In the CPS, final software testing was performed by the same person or group of persons who designed and programmed the modifications. Without an independent review/quality assurance group, there can be no assurance the modified program or system is performing as specified by the user and running in accordance with functional specifications.

In the PPI survey, program modifications on SunGard were not subject to final testing by an independent review/quality assurance group to ensure program modifications operated as intended and unauthorized changes were not introduced. PPI officials advised us PPI SunGard systems are being migrated to a client server environment. In the client server environment, independent testing/quality assurance is performed. Officials indicated all PPI SunGard systems would not be off the mainframe computer until 2003. We believe until the migration is complete, authorized system modifications, whether scheduled or unexpected, should be subject to independent review/quality assurance to ensure they are performing as specified by users.

We also found that computer programs were developed and written by PPI survey staff (economists/statisticians) in either FoxPro or Visual Basic programming language and were not subjected to an independent review/quality assurance to ensure the programs operated as intended and no unauthorized changes were introduced. These programs are used to enter, manipulate, sort, summarize and print sensitive data. Some of the programs process data on a continuous basis and are needed by the economists/statisticians to perform their jobs. Without subjecting these programs to independent review/quality assurance, there is no verification only authorized programs and modifications are implemented.

b. Access to Programming Source Code Was Not Restricted on the Mainframe Computer

We also found program source code library restrictions needed improvement to protect the source code from unauthorized access and accidental or deliberate destruction.

In the PPI survey, as is typical for the other surveys, data are processed on the mainframe and client server computer platforms. However, PPI survey computer programmers have access to the programming source code on the SunGard computer. Access to the production programming source code should be restricted to the programming staff authorized to work on the program source code. Access to software libraries should be protected by the use of access control software or operating system features and physical access controls. Furthermore, the movement of programs among libraries should be controlled by an organization segment independent of both the user and the programming staff to ensure software programs are protected from unauthorized changes.

c. Some Surveys Were Not Using a Standard Library Management System to Protect Software

Not all surveys were using a standard library management software package to protect their computer programs. These problems are discussed below by survey group.

In the CPS, we noted an absence of automated software inventory and version tracking tools. Such tools help prevent problems such as losing track of the most recent version or programmers overwriting each other's changes.

In the CPI survey, we found the programming development staff used manual procedures for tracking software changes (version control) to track the most recent version.

BLS responded to our Statement of Facts as follows:

> *For the CPS, the transfer of responsibility to FSMS for the design, development, and maintenance of CPS production systems will further ensure that CPS systems programming is conducted under standard OTSP procedures for systems development, testing, and use of tracking tools.*
>
> *For the CPI, systems staff investigated several automated tools and concluded that the manual procedures in place were superior to those offered by the automated tools.*

Recommendations

To improve management controls over survey applications software testing and protection, we recommend the Commissioner:

1. Require the independent review/quality assurance function be performed for all modifications before placing programs or systems into production.

2. Obtain and implement a standard library management system to protect software.

3. Restrict access to all programming source code.

BLS Response to the Draft Report

BLS' response is summarized below and numbered to correspond with OIG's recommendations. The complete text of BLS' response is contained in Exhibit I of this report.

1. Implementation should be completed by July 1999. Independent review/quality assurance will be required for all modifications before placing any programs or system into production.

2. Implementation is under way and deployment should begin by January 2000. OTSP has chartered a team to identify an appropriate standard library management system or systems.

3. Implementation is under way and should be completed in July 1999. Substantial restrictions to programming source code have long been in place. New restrictions will authorize only system librarians to move source code to and from production libraries.

OIG Conclusion

Based on BLS' response to our Statement of Facts and draft audit report, OIG considers the above recommendations to be resolved. The recommendations can be closed when BLS provides adequate documentation that the corrective action has been implemented.

4. Security Vulnerabilities Existed in the Local Area Network Infrastructure

Security vulnerabilities in the local area network (LAN) infrastructure could result in compromising sensitive data files. Our review of LAN operational controls disclosed the following deficiencies:

a. disaster recovery plan for continuous operation had not been tested for most BLS mission-critical systems and the IT security plan was incomplete;

b. servers in the BLS LAN subnet were not always secure;

c. controls over dial-in communication lines were inadequate;

d. terminated employees and contractors sometimes retained access to BLS computers;

e. inactive user accounts were not deleted;

f. encryption technology was not used to protect passwords as well as confidential and embargoed files;

g. policy for frequency of password changes was nonstandard; and

h. password protected screen savers were not used to protect unattended computer work stations.

These vulnerabilities existed because BLS had not conducted an OMB Circular A-130 systems security review of its LAN in the last 8 years. These vulnerabilities leave the BLS LAN susceptible to disruptions and unauthorized access.

BLS relies on its LAN to perform essential functions and meet mission goals. Consequently, strong, effective internal controls are needed to mitigate the risk of unauthorized disclosure of sensitive data and disruption of critical operations. Additionally, natural disasters and inadvertent errors can disrupt IT operations if assets are not adequately protected.

a. Disaster Recovery Plan for Continuous Operation Had Not Been Tested for Most BLS Mission-Critical Systems and the IT Security Plan Was Incomplete

BLS needs to be better prepared to prevent and respond to risks to its LAN. We found that disaster recovery plans for continuous operation had not been tested for most BLS mission-critical systems and the IT security plan did not fully address specific impacts of security threats and vulnerabilities. As a result, BLS may not be able to continue operation when unexpected events occur.

In the past year, BLS had tested only one (the International Price Index) of its 23 mission-critical systems for continuous operation. The CPI system was tested several years ago. The BLS Security Manager told us testing these systems is costly. However, BLS plans to test at least one more system by the end of 1999 and will schedule tests for all other systems as soon as practical.

Further, BLS stated meetings are being held with all systems managers to create Continuity of Operations Plans (COOP)/Disaster Recovery Plans for individual systems where there are none, and update the existing plans. Additionally, BLS stated they will verify the completeness of functions covered under the draft COOPs.

We also found the BLS IT security plan had not been revised recently as required. The plan needs to be immediately updated and periodically reviewed. Specifically, we found the plan did not fully address the impact of the following threats and related vulnerabilities:

- unauthorized access to the LAN and LAN resources;
- unauthorized disclosure or modification of data and programs;
- spoofing of LAN data (one user masquerading as another); and
- disruption of LAN functions.

BLS agreed and stated that the overall security plan has been well received by DOL and work is under way on adding specific security plan information.

b. Servers in the BLS LAN Subnet Were Not Always Secure

Improvements are needed in BLS policies and procedures to ensure consistency in the level of security over servers in the BLS LAN subnet. Our review of servers and backup media in the five survey offices disclosed they were not always physically secure and the server technical security controls were not always properly set up. Without adequate security, sensitive files in the servers are vulnerable to unauthorized access or misuse.

Current BLS IT policy appears to be inconsistent. According to BLS IT policy, the program survey office management is primarily responsible for the security of their servers. Program survey managers are responsible for identifying and implementing the controls necessary to safeguard BLS data processing environment. Yet, OTSP is delegated BLS-wide responsibility for setting policy concerning computer security implementation and management.

In our opinion, the above inconsistency results in the following server security vulnerabilities:

(1) Inadequate Physical Security Over Servers

At the CES, CPS, and PPI survey offices, we found servers located in open work areas. These servers were installed without consideration they could be vulnerable to damage, vandalism or unauthorized access. We also identified physically secured servers in these offices.

Physical security of the building in which BLS is located appears adequate. There are guards at all entrances and card keys are used by employees. The IT policy on physical security advises restriction of unauthorized access to servers can be accomplished by the use of card keys. Card keys can also be used to regulate individual access to a set of secured rooms within the building.

We found physical security was not adequate for 5 of 13 servers administered by the CES survey office and the single server administered by the CPS Division of Labor Force Statistics. The CES survey office servers were located in rooms in which access was not limited to only those staff that worked there. At the CPS survey office, we found the server was located in the general work area. At the PPI survey office, we found that servers were unattended in an unlocked office. We found this condition in the survey office and in the Division of Producer Price Systems in OTSP.

At the CPI and ECI survey offices, we found all servers were physically secure. The managers for these survey offices decided that locating all their servers in the ADP Center would provide uniform physical security. The ADP center used a card key pass system to limit access to only authorized staff. The ECI had a separate room within the ADP Center which was secured with a touch pad lock.

(2) Improper Storage of Backup Media

We found that all server administrators were performing data backups; however, the backup tapes were not always adequately stored. The IT security manual advises backup tapes should be kept away from the system under lock and key. If the data are mission-critical, the tapes should be sent to LAN Support for offsite storage.

At the CES and CPS survey offices, server administrators stored backup tapes in locked cabinets near the system. This is in contrast to the ECI survey office that backed up all servers at the same time and sent the backup tapes to BLS offsite storage. Thus, ECI would be in a better position to restore its data and programs in the event of a disaster. Currently, both the CES and CPS use the offsite mainframe computer to store a majority of its survey programs and micro data; however, both offices are going through major revisions to put their operations on a server platform. When these revisions are completed, offsite storage of backup tapes will be critical.

(3) Inadequate Technical Security Controls

We found problems with technical security controls. At our request, the BLS Security Manager used two security software packages (the Internet Security Systems Net Scanner and Dump ACL) to scan seven servers used to store embargoed data. The common problems identified by the security software packages were:

- locked accounts;
- user accounts never used;
- dormant and disabled accounts;
- user accounts with expired passwords;
- user accounts, including superusers, with passwords that will never expire;
- dummy accounts; and
- audit policies not requiring logging (audit) of use of user right and process tracking.

The above vulnerabilities can result in unauthorized access to the servers. All survey offices advised us they have corrected or will correct the problems.

The security software also identified a serious problem in one of the CES survey office's NT servers. No access permission controls had been set up for a backup folder which contained a file used to execute system backups. This could allow unauthorized access to the file and provide the unauthorized user the capability to change the file. By changing the file, the unauthorized user could execute any command desired. The survey office corrected the problem immediately after they were informed of it.

Although the BLS Security Manager did periodically test LAN subnet servers, we concluded the testing process needs to be strengthened. This can be achieved by requiring server administrators to test their technical controls on a regular basis and document vulnerabilities identified and the corrective action taken. The problem with no access permission controls occurred because the server administrator was not technically qualified. The server administrator was an economist, performing server administrator responsibilities under "other duties as assigned." OTSP LAN Support had to set up the server when it was installed. BLS' practice of relying on server administrators who do not have an IT background can cause problems.

In the ECI survey office, a server administrator receives requests for directory creation and permissions, and forwards them to another server administrator in OTSP for implementation. The OTSP server administrator is an IT specialist.

Overall, we concluded BLS needs to strengthen its existing IT policies to require more OTSP involvement in server security. BLS should require servers be located in secure rooms with limited access. Additionally, BLS should require survey offices to establish a position for a qualified individual to be responsible for security oversight of all its servers.

c. Controls Over Dial-in Communication Lines Were Inadequate

BLS headquarters had over 2,600 dial-in communication lines. We concluded dial-in communication line management should include the IT security team. Until recently, additional lines were installed based on a request from the cost center manager with no review of the request by the IT security team. Without adequate control over these lines, the LAN is vulnerable to unauthorized access.

The BLS security team identified dial-in communication lines as a potential vulnerability. Effective March 9, 1999, BLS instituted significant changes in its lines management policies. The new policy requires the IT security team to review and certify any new line requests. The policy also requires each manager to justify all existing lines to the satisfaction of the IT security team.

BLS responded to our Statement of Facts as follows:

> *The BLS does not install a line unless requested by a Cost Center Manager. The BLS generally reviews its lines each year. . . . Following the OIG's attention to this matter, OA and OTSP are taking extra steps to ensure that it is addressed fully. Requests for new data lines now will be granted only upon approval of the IT Security Officer.*

d. Terminated Employees and Contractors Sometimes Retained Access to BLS Computers

We obtained printouts of employees and contractors who separated from BLS during the period November 1, 1998 through February 18, 1999. We also obtained listings of the users having currently open Windows NT and SunGard computer accounts. We compared the printouts of valid computer accounts with separated workers.

This review disclosed that at least 14 separated employees and contractors still had valid Windows NT client server accounts and passwords and at least 11 employees and contractors still had a valid SunGard account after their termination.

The cause of the security problem is flawed communication between the personnel department and LAN support and SunGard support.

OIG concluded this was a serious security problem. As one BLS LAN contractor stated, "these ex-employees/contractors could wipe us out if they wanted to."

BLS should review the existing computer accounts and verify each account should be kept active.

OTSP management stated they handle hostile terminations different from normal terminations. For employees terminated under hostile conditions, their ID cards are confiscated immediately, their computer accounts disabled/deleted and they are escorted out of the building. Non-hostile terminations are processed using BLS' normal terminations procedures; i.e., BLS personnel department notifies the BLS office responsible for deleting/disabling the terminated employee's computer accounts.

BLS responded to our Statement of Facts as follows:

> *A distinction should be made between separated and terminated (dismissed) employees. As noted in the OIG report, extra precautions are taken to ensure that accounts are deleted immediately for terminated employees. The BLS agrees that improvements are needed in its process to delete SunGard accounts upon separation of employees and contractors. Corrective action is underway. After an initial effort is completed to identify and eliminate accounts that should be deleted, the BLS then will reconcile all remaining accounts with personnel listings and/or verify system accounts with Division Chiefs.*
>
> *The BLS also will work to ensure that the employee notification process works efficiently and reliably. Also, BLS will review the list of persons who receive notification of separations and ensure that the appropriate administrators of BLS Windows NT and Unix systems are included. The BLS IT Security Team will conduct regular audits to ensure that accounts are deleted in a timely manner.*
>
> *An important point regarding this matter is not included in the OIG report. The existence of an account for a separated employee is not necessarily an indication that the employee still has access to the account. Before the account of a separated individual is deleted, passwords are required to be changed promptly in both the client server and mainframe environment. The existence of account initials is not sufficient for access without a password. This practice is necessary because account initials may be needed by the BLS to access files created by the separated individual.*

e. Inactive User Accounts Were Not Deleted

We requested a report showing the number of days that had passed since the last logon for each BLS Windows NT user. Our analysis of account activity established that 20 percent (317 of 1,615) of the user accounts on the Postal Square Building (PSB) subnet had never been used. We also identified another 16 accounts which had not been used for more than one year. After reviewing the report, BLS deleted the inactive accounts.

We concluded that BLS is not reviewing user accounts for inactivity. BLS should review all user accounts on all computer systems to identify and delete inactive accounts.

BLS agreed they were not reviewing user accounts. OTSP/LAN management started reviewing user accounts to identify and deactivate inactive accounts. This analysis will continue throughout BLS. In addition, the IT security team will periodically confirm these reviews.

f. Encryption Technology Was Not Used to Protect Passwords as well as Confidential and Embargoed Files

Encryption technology was not used on all BLS computer systems to protect passwords and confidential and embargoed files. On the NT servers, some passwords and files are encrypted; however, the UNIX servers and SunGard do not have encrypted passwords or files. BLS IT management advised us encrypting passwords on all LAN servers containing sensitive information would be cost prohibitive.

Hacking into BLS LAN or internal employee misuse or sabotage of sensitive data could cause a disruption of network functions or unauthorized disclosure of sensitive data. This could jeopardize the credibility of BLS published economic and statistical data with the public and affect national monetary systems such as banks and stock markets. In our opinion, data and files stored on the BLS LAN and at SunGard demand protection which mandates encryption be used even when other access controls are considered adequate. Further, encryption takes on additional importance because BLS information requires a high level of confidentiality.

BLS responded that they are dedicating funding for the inclusion of switching mechanisms throughout the LAN rather than for encryption software. Although installing hardware switches between subnets with sensitive data stored on them will decrease vulnerability from Internet hacking outside the BLS firewall, we believe the LAN is still vulnerable to misuse of sensitive data and sabotage from within by employees and contractors.

g. Policy for Frequency of Password Changes Was Non-Standard

Current BLS policy requires passwords be changed every 6 months. According to Federal Information Processing Standards, passwords protecting sensitive data should be changed every 30 days.

BLS servers contain sensitive data which must be protected. We believe BLS should require changing passwords every 30 days.

BLS disagrees with OIG's position on changing passwords, and responded to our Statement of Facts as follows:

> *Requiring users to change their passwords every 30 days would likely result in users writing their passwords on paper because they would have trouble remembering their frequently-changed password. This would be a greater security risk than continuing to allow users to keep a password for up to 6 months.*

h. Password Protected Screen Savers Were Not Used to Protect Unattended Computer Work Stations

At the CPI and PPI survey offices, we found password protected screen savers were not used to secure unattended personal computers. When computer terminals were unattended, a screen saver would activate after a set number of minutes. The screen savers were not password protected. Therefore, any files or programs accessed would be displayed whenever any key on the terminal was touched, or the mouse was moved. This practice potentially would allow unauthorized users to access BLS files.

BLS agreed to require the use of screen saver passwords. BLS stated:

> *OTSP has instituted its BLS-wide policy that use of screen saver passwords is mandatory. This already has been published informally, and will be implemented in the near future.*

The problems identified above demonstrate the BLS LAN infrastructure may be vulnerable to unauthorized access, inappropriate use of BLS sensitive data, and disruption of critical operations.

Recommendations

To strengthen LAN security, we recommend the Commissioner:

1. Test the continuity of operations in all BLS mission critical systems.
2. Update and periodically review the BLS IT security plan.
3. Require each server administrator to periodically test and ensure technical security controls are adequate.
4. Develop and implement IT security procedures to require all servers and backup media be located in a secure location with limited access.
5. Require each survey office to establish a position for a qualified individual to be responsible for security oversight of all its servers.
6. Strengthen controls over data lines by implementing procedures to require all requests for data lines be justified and be reviewed by the IT security team.
7. Identify and review all existing data lines to ensure they are needed.
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.
9. Improve IT security by installing software to encrypt passwords on servers where the passwords are stored and before one-way transmission from point-of-entry to point-of-authentication.
10. Encrypt confidential and embargoed files wherever possible.
11. Require password changes every 30 days.
12. Require screen saver password protection for all workstations.

BLS Response to the Draft Report

BLS' response is summarized below and numbered to correspond with OIG's recommendations. The complete text of BLS' response is contained in Exhibit I of this report.

1. Continuity of Operations Plans (COOPs) for all mission-critical systems should be developed by January 2000, and testing of critical systems that produce a Principal Federal Economic indicator should be completed by January 2002. The costs and staff time involved in testing a COOP prohibit BLS from quickly testing all plans in a short time frame. Testing for LABSTAT should be completed by June 2002.

2. A risk analysis should be completed by the end of Calendar Year 1999, and the IT Security Manual will be updated as appropriate. Additionally, an updated A-123/130 review plan should be finalized in July 1999.

3. Implementation should be completed by October 1999. BLS will institute a quarterly certification process, which will require server administrators to submit a completed security checklist to the IT Security Team for review.

4. OTSP has chartered a team to review the physical location and logical administration of all servers within BLS. Upon completion of the review, BLS will make and implement decisions on the physical location and security of servers and backup media.

5. BLS will ensure that individuals assigned the responsibility for server administration and security receive adequate training. Implementation should be completed by July 2000.

6. All National Office requests for data lines now must be approved by the IT Security Team. An appropriate clearance for regional offices requests should be in place by September 1999.

7. An inventory of data lines in the National Office was completed in June 1999, and unused data lines were eliminated. The same procedure should be completed in regional offices by October 1999.

8. Deletion of Separated Users' Accounts - Network and subnetwork administrators will be informed of BLS employee and contractor separations. Separated employees' and contractors' account passwords will be changed, and the accounts will be deleted within 20 business days. This procedure should be in place by October 1999.

Deletion of Inactive Accounts - On the first business day of each month, accounts will be checked that have not been accessed within the last 30 days, and inactive accounts will be deleted within 20 business days. This procedure should be in place for NT accounts by July 1999 and October 1999 for UNIX accounts.

Management Review of Accounts - Managers will be required to verify computer accounts annually in October. Accounts not identified as active by the last business day in October will be disabled and deleted within 20 days. This procedure should be in place in July 1999.

9. An evaluation is under way to determine if BLS can fully implement OIG's recommendation to encrypt passwords. Implementation should be completed as fully as possible by July 2000.

10. Work is under way to determine the extent to which BLS can encrypt confidential and embargoed files, and expanded use of encrypted files should be implemented by July 2000.

11. BLS plans to require passwords be changed every 90 days instead of every 180 days as is currently being done. The NSA report recommended passwords be changed every 90 days, and 90 days is within the range of GAO's guidelines. BLS believes that requiring passwords be changed every 30 days would increase security vulnerability because users would more likely write their passwords down to remember them. The change in password policy should be implemented by October 1999.

12. BLS has established a policy requiring that password protected screen savers be enabled on all workstations and servers, and that a maximum inactivity time of 15 minutes be used. Automated methods for auditing and enforcement are being developed.

OIG Conclusion

Based on BLS' response to our Statement of Facts and draft audit report, OIG considers the above recommendations to be resolved except for numbers 9 and 10. We continue to recommend that BLS encrypt all passwords and all confidential and embargoed files. While we also continue to believe passwords should be changed every 30 days as called for by Federal Information Processing Standards, we are resolving recommendation number 11 because 90 days is within GAO's guidelines. The resolved recommendations can be closed when BLS provides adequate documentation that the corrective action has been implemented.

Chapter II Inconsistent Security Practices in Program Survey Offices

The security practices and the level of security varied among the five survey offices we audited. BLS needs to ensure comprehensive security practices for preparing and disseminating news releases involving embargoed data are developed for and then followed by program survey offices.

We found the following conditions in one or more of the five survey offices:

1. procedures for preparing and disseminating news releases were incomplete and out of date;
2. news releases were prepared in unsecured work areas;
3. procedures for protection, destruction and number of copies of sensitive reports were inconsistent;
4. practices protecting electronic files containing sensitive data were not consistent; and
5. policies and procedures for employees who work at home (flexiplace) were insufficient.

These conditions occurred because BLS, until recently, had not established centralized news release security standards and practices. As a result, there was no assurance all security vulnerabilities were addressed to protect against the unauthorized use and/or disclosure of sensitive news release data.

We reviewed the security policies and procedures in effect for five survey offices. We also reviewed Office of Publications and Special Studies' (OPSS) procedures for disseminating news releases via "the fax on demand system."

Overall, we concluded that BLS employees and managers were aware of the importance of news release security controls and the need to protect BLS confidential and embargoed data from unauthorized access or prerelease. We found that before the November 1998 and January 1999 prereleases, two survey offices performed internal security reviews of the news release process. This demonstrated these survey offices took data security seriously. Security awareness has been heightened since the two prereleases. Additionally, the survey offices were receptive to correcting the security vulnerabilities we identified during our audit.

We concluded OPSS had effective policies and procedures for the security over the “fax on demand” news release process.

Our audit of security in the five survey offices disclosed that although many controls were in place, the level of security varied and vulnerabilities existed. The following details are provided.

1. Procedures for Preparing and Disseminating News Releases Were Incomplete and Out of Date

None of the five survey offices reviewed had a comprehensive policies and procedures manual for preparing and disseminating news releases. We found written procedures that did exist were fragmented among the individuals involved in producing the news release. Without a comprehensive policies and procedures manual, survey office managers do not have a frame of reference for administering security, and employees do not know what is expected of them.

Formal policies and procedures provide greater assurance that specific instructions are communicated to the news release staff. They can be used to remind employees of their responsibilities and to provide standards for measuring employee performance (compliance).

In response to the latest prerelease incident, the BLS Commissioner issued instructions to all Associate Commissioners to have their survey offices document all processes and procedures for preparing and disseminating news releases. The instructions called for identifying fundamental security principles the survey offices should ensure are incorporated into processes and procedures. This initiative, when completed, should provide the survey offices an adequate basis for developing a comprehensive policies and procedures manual for each news release involving embargoed data.

BLS responded to our Statement of Facts as follows:

> *Prior to the November and January prerelease incidents, the BLS procedures documentation was in various states of completeness and were not always current. Following the incidents, the Commissioner established a Security Steering Committee and a Security Review Team to conduct a comprehensive review. The Security Review Team developed a number of fundamental security principles that should be followed in the preparation and distribution of embargoed data. The Commissioner directed every BLS program to submit complete, up-to-date process documentation incorporating those principles where applicable. Nearly all BLS programs have submitted this documentation and all programs will complete this task in a timely manner. The*

respective documentation will be distributed to BLS staff involved in prerelease processing. Additional work is required to make the documentation fully complete, and to keep it current. The BLS will add a periodic review and evaluation capacity to ensure adequate documentation of procedures on an ongoing basis.

Recommendations

We recommend the Commissioner:

1 Develop BLS-wide security standards to be followed by survey offices.

2. Ensure comprehensive policies and procedures manuals are developed for preparation and dissemination of sensitive news releases.

BLS Response to the Draft Report

BLS' response is summarized below and numbered to correspond with OIG's recommendations. The complete text of BLS' response is contained in Exhibit I of this report.

1. BLS will issue a Commissioner's Order on management control and data security and an Administrative Procedure on data security standards by October 1999.

2. A Data Security Steering Committee and Data Security Review Team were formed in February 1999 and is reviewing the security of sensitive news releases. Offices involved in preparing and disseminating embargoed data documented their processes for review by the Security Review Team. Any necessary improvements will be made, and new security standards are being developed.

OIG Conclusion

Based on BLS' response to our Statement of Facts and draft audit report, OIG considers the above recommendations to be resolved. The recommendations can be closed when BLS provides adequate documentation that the corrective action has been implemented.

2. News Releases Were Prepared in Unsecured Work Areas

We found varied levels of physical security over the individual office areas where the news releases were prepared. The PPI and CPI offices did not secure office areas to limit access to only those employees who worked there. These office areas were vulnerable to access by unauthorized individuals.

The CPS, CES and ECI survey offices had adequate physical security and recognized operating in an open environment posed risks to security over news release data. These survey offices locked the doors to work areas when the news release was being prepared. Only employees who worked in the survey office could access the office area.

The CES, and recently the ECI, survey offices consolidated their respective news release staffs into one location and secured it using the card key security system. This kept staff not involved in the news release process from having access to embargoed data and documents.

The PPI survey office now locks all doors to its office area and have advised us they plan to consolidate their news release staff in one location. The CPI survey office management has told us they plan to start securing their area in May 1999.

BLS responded to our Statement of Facts as follows:

> *Effective immediately, the BLS program offices that process Employment Situation, ECI, PPI, and CPI embargoed data will lock entrance doors during the preparation of those data. Furthermore, the BLS will consider the feasibility of reconfiguring office space to physically separate program office staff who process those data.*

Recommendation

We recommend the Commissioner ensure work areas for preparation of news releases are segregated and secure.

BLS Response to the Draft Report

BLS responded that all BLS Principal Federal Economic Indicators now will be released through the Department of Labor “lock-up” procedure. Advance copies of these releases will be printed in the Postal Square Building rather than at the Department of Labor Print shop. Physical access to areas where these data are present will be restricted to authorized individuals, and “restricted access” signs will be placed at entrances to those areas. These actions should be completed by November 1999.

Over the long-term, the BLS will consider the advisability and feasibility of reconfiguring office space to segregate staff working on these releases. BLS may conclude, however, that alternative measures can be used to achieve the appropriate level of security.

OIG Conclusion

We continue to recommend that news releases be prepared in work areas that are segregated and secure. This recommendation is not resolved.

3. Procedures for Protection, Destruction and Number of Copies of Sensitive Reports Were Inconsistent

Not all survey offices in our review adequately protected and/or destroyed documents containing embargoed and confidential data. These offices did not have an effective system in place to ensure confidential and sensitive materials were always securely stored and properly destroyed when no longer needed. Some survey offices produced excessive copies of reports containing embargoed and confidential data. This led to the following conditions:

a. Sensitive Reports Were Not Disposed of Properly

Although BLS employees generally handled confidential respondent data appropriately, there were vulnerabilities in the disposal of documents containing such information for two survey offices.

At the PPI survey office, we found printouts containing confidential respondent data were not always disposed of properly. We were told these printouts were sometimes placed in a recycling stack along with newspapers and nonconfidential printouts. We also observed a large stack of confidential printouts and newspapers awaiting recycling next to a doorway. Our cursory review of these printouts showed they contained confidential information such as establishment names and addresses, value of shipments, sample employment, items sampled, item prices, etc. The survey office did not have a system to ensure that such printouts were sent to the shredding facilities located in the computer print shop. PPI survey office management informed us they recently purchased two lockable containers for storing documents to be shredded.

At the ECI survey office, we found during the process of reviewing reports containing preliminary estimates, several "working copies" were produced and used by the reviewers. We were told these "working copies" were disposed of by placing them in the recycling container. In our opinion, these "working copies" should have been shredded. Even though these reports did not show respondent names, they did show schedule numbers which could be used to identify respondents if the right coding was obtained.

We were told by ECI survey office management these "working copies" should be treated as confidential. The ECI survey office plans to purchase an additional shredder and a secure bin for confidential material. Additionally, staff will be briefed in detail on the importance of the proper handling of sensitive materials and management follow-up procedures will be put in place.

BLS responded to our Statement of Facts as follows:

> *. . . BLS agrees with OIG that procedures for controlling, protecting, accounting for, and destroying computer printouts containing sensitive information/data need to be improved. The Office of Administration is re-educating all BLS offices of the process in place for the destruction of printouts containing sensitive information and data. A memorandum providing guidelines, responsibilities, and options available to programs for disposing of sensitive materials is now being drafted for distribution to all cost center managers. Program offices are being instructed to procure secure/lockable containers as needed for storing sensitive materials prior to destruction.*

b. Reports Containing Embargoed Data Were Not Properly Controlled

There were security weaknesses in the control over computer printouts containing embargoed data printed in the ADP center for three survey offices.

In the CES survey office, we found the chain of custody over printouts was jeopardized because they were delivered by mail room staff rather than being picked up by survey office staff. Although the survey office tracks the scheduled delivery of the printouts, we still consider this a security weakness because of the sensitivity of the data.

In the PPI survey office, we found computer printouts containing embargoed data printed by the ADP center were not tracked. We were told by the survey office staff there have been occasions when the printouts were never received. The staff assumed that the printouts were misdelivered to other users who did not bother to forward them. We found there were no procedures covering the delivery and accounting for the printouts.

In the CPI survey office, we found a control procedure needed to be changed and enforced. The procedure required ADP center staff maintain a control sheet for sensitive printouts when they are placed into a safe. However, this procedure did not identify each print job submitted. Having the requestor initiate the control sheet will allow the control sheet to be reconciled with the printouts. During our observation of the handling of the printouts by the ADP center, we noted the safe was not locked as required by written procedures.

BLS responded to our Statement of Facts as follows:

> *Effective immediately, designated program office employees will transport all printouts that contain embargoed data from the ground floor ADP center to the appropriate program office, or will accompany personnel assigned to transport the listings. All embargoed listings will be placed in a locked bin in the ADP center until the designated employees retrieve them.*

c. Excessive Copies of Sensitive Documents Were Produced

Two survey offices generated excessive copies of computer printouts containing confidential and embargoed data. This created problems in the proper disposal of printouts.

The PPI survey office constantly generated a high volume of printouts containing confidential data. Due to the sheer volume of the printouts, they could not be secured in locked cabinets. Additionally, the large volume of paper makes proper disposal by shredding more difficult. PPI survey office management responded that a new electronic collection process would help reduce the amount of paper generated. In addition, using a shared directory to store price notes would avoid the unnecessary printing of the information.

At the CPI survey office, we found multiple copies of documents containing sensitive information were unnecessarily printed and distributed. The documents contained price notes describing changes in prices of products in industries. Rather than printing price notes, placing them in a shared directory accessible only to those employees with a need to know prior to the news release would reduce the chances sensitive data could be prematurely released. CPI survey office management informed us they will place the price notes in a limited access, shared directory.

Recommendation

We recommend the Commissioner strengthen and enforce policies and procedures for safeguarding printouts with confidential and embargoed data.

BLS Response to the Draft Report

A memorandum to all BLS employees is being prepared to remind them that confidential printouts must be treated in a secure manner, excessive printing of confidential listings should be avoided, and to inform them of facilities available for disposal of confidential materials. Triennial application security reviews will assess the security of confidential printouts. Physical security controls for the ground floor computer center will be improved by January 2000. A sign has been posted stating that central LAN printers should not be used for printing sensitive or embargoed data.

OIG Conclusion

Based on BLS' response to our Statement of Facts and draft audit report, OIG considers the above recommendation to be resolved. The recommendation can be closed when BLS provides adequate documentation that the corrective action has been implemented.

4. Practices Protecting Electronic Files Containing Sensitive Data Were Not Consistent

We found the survey offices used different methods to store electronic files that contained embargoed data. Uniform procedures need to be implemented.

According to BLS policy, employees are not to store sensitive data on their PC. The sensitive data should only be stored on a server. This is required because of the low level of security provided by the Windows 95 Operating System.

Three survey offices recognized that using shared directories on servers can limit the access of sensitive files to only authorized individuals. The ECI survey office policy stated shared directories eliminate the use of e-mail in the transferring of files among staff.

We found the CPI and CPS survey offices did not always use servers to store embargoed data. Instead, these survey offices stored embargoed data on PCs or floppy disks. The floppy disks were then stored in a locked desk. These survey offices did not use servers because they were concerned about the level of security they provided. Based on our review of servers used for preparing news releases, we share this concern. However, this can be corrected if BLS strengthens its security management of servers.

Survey offices need to ensure sensitive electronic files are secured. It is our position this can be achieved by storing files on secured servers in which access is limited to authorized staff.

BLS responded to our Statement of Facts as follows:

> *As currently worded, [this finding] indicates that it applies BLS-wide. The audit observations cite only rare instances where this has occurred. However, all personnel who handle embargoed data will be instructed as to the existing requirement not to store sensitive data on C-drives. In the instances cited by the OIG, the BLS already has taken corrective action.*

Recommendation

We recommend the Commissioner strengthen and enforce policies and procedures for protecting electronic files containing sensitive data.

BLS Response to the Draft Report

BLS responded that storing sensitive data on computer C-drives has been discontinued except where the computer is in a locked room used only by employees preparing sensitive news releases. Storing sensitive data on diskettes is being reevaluated and discontinued where appropriate.

OIG Conclusion

Based on BLS' response to our Statement of Facts and draft audit report, OIG considers the above recommendation to be resolved. The recommendation can be closed when BLS provides adequate documentation that the corrective action has been implemented.

5. Policies and Procedures for Employees Who Work at Home (Flexiplace) Were Insufficient

Some employees participate in the flexiplace program and can work at home. Employees can access the BLS computer systems from home and perform the same tasks they can perform from their office workstations.

Employees must have MacAfee virus protection software on their home computers before they are allowed access to the BLS computer system.

Formal detailed written security procedures have not been developed for employees using flexiplace. Policies and procedures should be prepared to address whether employees can take confidential or sensitive data home or access it through their home computers. The procedures should also cover issues such as receiving or sending e-mail, whether home computer software must meet BLS standards, and storing information on the home computer.

The U.S. Department of Labor, American Federation of Government Employees - Local 12, Flexiplace Agreement, Article 10, provides that employees on flexiplace are obligated to apply necessary safeguards to protect government records from damage or unauthorized disclosure. The Individual Flexiplace Work Agreement also provides that employees will apply approved safeguards to protect government records from unauthorized disclosure, and will comply with Privacy Act requirements and agency confidentiality requirements. BLS confidentiality requirements include Commissioner's Order 3-93 and BLS Administrative Procedure No. 1-96. Neither of these BLS directives specifically addresses flexiplace issues.

BLS responded to our Statement of Facts as follows:

> *The BLS agrees that its flexiplace policies and procedures, with regard to data security, need to be improved. The BLS will strengthen and document those policies and procedures, including a prohibition against storing or printing sensitive data at home. The BLS does provide virus protection for computers used by flexiplace employees. The BLS will work with all flexiplace employees to have the latest virus protection software installed on their computers. Flexiplace employees are not permitted to take prerelease data home or access prerelease data from home. Contractors are not permitted to have flexiplace arrangements.*

Recommendation

We recommend the Commissioner establish flexiplace policies and procedures which address data security requirements.

BLS Response to the Draft Report

BLS responded that proposed flexiplace policies and procedures addressing data security requirements have been drafted and are currently being evaluated by senior management. Final policies and procedures should be issued by September 1999.

OIG Conclusion

Based on BLS' response to our Statement of Facts and draft audit report OIG considers the above recommendation to be resolved. The recommendation can be closed when BLS provides adequate documentation that the corrective action has been implemented.

Chapter III Deficient Personnel Security and Management Control

We audited administrative controls over personnel security and management control actions. We also looked at BLS follow-up on corrective actions taken on findings identified in prior reviews.

We identified the following deficiencies:

1. inadequate personnel security for employees and contractors;

2. employees who handled embargoed data were not provided periodic training or guidance on ethics and investment restrictions; and

3. BLS management control plan was incomplete.

Given the sensitivity of the information maintained at BLS, management should act to regularly reinforce the importance of data security to staff. Additionally, management controls must be in place to ensure that security practices are consistently applied. The following details pertain to the deficiencies identified.

1. Inadequate Personnel Security for Employees and Contractors

BLS did not have a consistent, comprehensive personnel security program. This is evidenced by the fact that:

a. many employees having access to embargoed (sensitive) data did not have background investigations;

b. the sensitivity of many positions was improperly classified;

c. background investigations were not updated as required; and

d. contract employees lacked security checks and background investigations.

Many employees in BLS handle sensitive economic data which may affect or predict financial market activity. An employee with advance knowledge of economic changes could potentially profit by making speculative investments, attempting to capitalize on anticipated market reactions.

The lack of a consistent, comprehensive security program may lead to a breakdown in the professional discretion BLS staff must exhibit in the area of personal investments. Additionally, any suspicion of actual or perceived breaches in BLS confidentiality of private employers' data may have an impact on their willingness to be involved in BLS programs, which could be devastating to the agency.

a. Many Employees Having Access to Embargoed (Sensitive) Data Did Not Have Background Investigations

All newly hired BLS employees are required to have a National Agency Check and Inquiry (NACI). This check is performed by the Office of Personnel Management (OPM) and costs about $74. The NACI includes a fingerprint, employment and education check. We found BLS to be in compliance with this requirement.

The Federal Personnel Manual (FPM) contains requirements for various levels of background investigations for employees in critical or sensitive positions. Every employee having access to sensitive data is required to undergo either a Background Investigation (BI), Limited Background Investigation (LBI), or Minimum Background Investigation (MBI), depending on the position risk level (sensitivity level).

We reviewed documentation on the security clearances for 58 employees who have access to embargoed data. We focused on employees who were responsible for preparing, reviewing or disseminating news releases for the CPI, ECI, PPI and Employment Situation Report.

Of the 58 employees, there was no documentation 33 of the employees had received any type of background investigation. Some of these employees have had access to sensitive information for many years.

According to BLS staff, some background investigations were inadvertently not done due to “oversights.” Some employees may not have completed and returned the required forms. There was no documentation of follow-up or management action to ensure requested background investigations were completed.

The number of background investigations not completed and the length of time some have been overdue point to a lack of management controls in this area. It also indicates that supervisory staff does not monitor the background investigation status of their employees. Even with management controls, the personnel system could not have been used to determine the need for security clearances due to position sensitivities being improperly classified, as discussed in the next section.

New software is being introduced which will be used for management of the DOL personnel system. The software (PeopleSoft) will be used to track security clearance information and position sensitivity. However, unless management (1) properly identifies the sensitivity of positions, (2) accurately indicates the security clearance status of personnel, and (3) actively monitors for required clearances being obtained, the new system will be of limited use.

BLS responded to our Statement of Facts as follows:

> *All security clearances have been initiated for those persons identified in the OIG audit as not ever having received the appropriate level of background investigation.*

b. The Sensitivity of Many Positions Was Improperly Classified

The current DOL personnel system, which contains security review information, does not properly identify the sensitivity of most positions that have access to embargoed data. The position sensitivity classification was incorrect for most of the employees we reviewed. This improper classification makes the system useless in monitoring the status of the proper security clearances for staff.

One employee was shown on a security listing to be in a non-sensitive position, yet holding a top-secret security clearance. The position should have been classified as critical-sensitive. The employee's security clearance record in his personnel file did not indicate any type of security clearance. We checked with the DOL Security Officer and found the employee had received a BI and held a Confidential security clearance.

Unless positions are appropriately classified, it is impossible for management to track who needs security clearances. The first step is to identify positions that require clearances; then determine if the individuals occupying the positions have the required clearance.

BLS responded to our Statement of Facts as follows:

> *The BLS will designate position sensitivity for all employee and contractor positions in accordance with the latest OPM guidance, and the appropriate security clearances will be performed on all employees and contractors who have access to embargoed data or work in critical areas.*

c. Background Investigations Were Not Updated as Required

Reinvestigations are required by the FPM every 5 years for employees in positions requiring a BI. We found for those staff who did receive a BI, most were not reinvestigated every 5 years.

Of the 58 employees we reviewed, 25 of them had proof of a background investigation in their files. However, according to file documentation, 20 of these 25 employees had background investigations more than 5 years ago.

We focused our review on employees who routinely had access to and review embargoed data. However, our review of the agency-wide security listing showed other employees in critical positions with outdated background investigations. For example, according to the listing, one senior manager's most recent background investigation was in 1972. A review of the employee's file revealed a more recent background investigation dated May 23, 1983. However, under a 5-year cycle, updated background investigations were due in 1988, 1993, and 1998.

This lack of background investigation updates points to a lack of management control and oversight.

BLS responded to our Statement of Facts as follows:

> *The OPM reinvestigation requirement is being deleted in the newest revision of the Code of Federal Regulations, part 731, pertaining to Suitability of Federal personnel positions. The regulations are due to be released in the spring of 1999.*

d. Contract Employees Lacked Security Checks and Background Investigations

Although contractors work alongside BLS employees and perform many critical functions, background investigations for them were rarely obtained. Also, even though all new BLS employees undergo an NACI security check, the process was seldom applied to contract employees. We found only 1 of 56 contractors performing central LAN support for the BLS in the National and Regional Offices had received a background investigation.

BIs may be required according to contract requirements, but are only initiated at supervisors' discretion.

The BLS LAN Services contract contains the following background investigation requirement for certain key positions:

> *Successful clearance of field background investigation by the Office of Personnel Management within one year of starting work on this contract. The Government will initiate such a background investigation as soon as practicable.*

The contract contains the following background investigation provision for all other positions:

> *The Government may require successful clearance of a field background investigation by the Office of Personnel Management within one year of starting work on this contract. If so required, the Government will initiate such a background investigation as soon as practicable*.

In 1994, 1996, and August 1998, the LAN services supervisor sent memoranda to the BLS personnel office requesting background investigations for six contractors. Only one of the background investigations was completed. There was no documentation of follow-up or any action on the part of management to determine why the requested clearances were not obtained.

We reviewed a November 1994 GSA Physical Security Survey Report on the Postal Square Building that houses BLS. According to the report:

> *There is a requirement for security background checks to be conducted on the contracted and janitorial employees working in the Department of Labor space within this facility.*

BLS janitorial services are obtained through a GSA contract. GSA is responsible for arranging security clearances for janitorial contract staff. Part of the rationale for requiring security clearances may be because janitorial staff often work during non-business hours when other staff is not present. However, we believe it is inconsistent that janitorial contract staff would be required to undergo background checks, while computer contract staff is not required to have security clearances.

BLS responded to our Statement of Facts as follows:

> *The BLS will establish and implement a policy requiring contractors to have the appropriate security clearance based on established guidelines consistent with Federal service employee positions.*

BLS provided us an internal draft Personnel Security Review report dated April 6, 1999. This report states many of the personnel security problems OIG identified and provides recommendations for corrective action.

Recommendations

To improve controls over personnel security, we recommend the Commissioner:

1. Ensure the sensitivity level for all positions is accurately classified.
2. Ensure appropriate security clearances are obtained for all employees in critical or sensitive positions.
3. Ensure NACI checks are performed for all contract staff and appropriate security clearances are obtained for all contract staff performing critical or sensitive duties.
4. Ensure procedures are instituted to continually monitor the sensitivity of position classifications and employee and contractor security clearances.

BLS Response to the Draft Report

BLS responded that they will conduct a thorough review of all employee and contractor positions and will update position risk designations in accordance with the latest OPM guidance. Then, based on the position risk designations, BLS will initiate appropriate security checks/clearances (NACI at a minimum) for all employee and contractor personnel as necessary. Procedures will be put in place to ensure that appropriate security checks/clearances are performed on all new employee and contractor personnel, and on personnel who change positions within the BLS. All of these actions should be completed for personnel who work with prerelease data for the Principal Federal Economic Indicators by January 2000, and for all other personnel by April 2000.

OIG Conclusion

Based on BLS' response to our Statement of Facts and draft audit report, OIG considers the above recommendations to be resolved. The recommendations can be closed when BLS provides adequate documentation that the corrective action has been implemented.

In our draft report we discussed that certain background investigations were not always updated every 5 years as required by the Federal Personnel Manual. BLS' response to our Statement of Facts stated that the OPM reinvestigation requirement was being deleted in revised regulations due to be released in the spring of 1999. Consequently, our draft report did not recommend that reinvestigations be performed. However, the revised regulations have yet to be issued. If the reinvestigation requirement is not dropped by OPM, BLS should take appropriate action to update background investigations as required.

2. Employees Who Handled Embargoed Data Were Not Provided Periodic Training or Guidance on Ethics and Investment Restrictions

Most BLS employees do not receive periodic training or reminders of governmental ethics guidelines and investment restrictions. Only Senior Executive Service employees receive annual ethics training and file annual financial disclosures even though many other staff handles sensitive and confidential information.

Many BLS employees have access to sensitive economic data before it is released to the general public. An employee with advance knowledge of economic changes could potentially profit by making speculative investments attempting to capitalize on anticipated market reactions.

Investment restrictions are contained in the government-wide publication *Standards of Ethical Conduct for Employees of the Executive Branch,* dated August 1992. All new employees are provided the Office of Government Ethics (OGE) handbook and attend an ethics orientation presentation. Subpart G – Misuse of Position, Section 2635.703, Use of Nonpublic Information, contains the following restriction regarding using sensitive information to personal advantage:

> *(a) Prohibition. An employee shall not engage in a financial transaction using nonpublic information, nor allow the improper use of nonpublic information to further his own private interest or that of another, whether through advice or recommendation, or by knowing unauthorized disclosure.*

BLS requires all non-BLS employees, having access to confidential records, to sign a Non-Disclosure Affidavit. The affidavit provides that the economic series data prepared for release to the public shall not be disclosed or used in an unauthorized manner before their official dates and time of release, and shall be accessible only to authorized persons.

All BLS employees must sign an acknowledgment letter certifying that they have read the three following directives:

(1) Administrative Procedure 1-96, “Responsibility for Safeguarding Confidential Information,” spells out employees’ responsibilities, including never divulging prerelease estimates to any individual who is not an authorized person.

(2) Commissioner’s Order 3-93, “Confidential Nature of BLS Records,” which states that prerelease economic series data prepared for release to the public will not be disclosed or used in an unauthorized manner before being cleared for release.

(3) Commissioner’s Order 1-96, “Consumer Price Index Futures Contracts,” which prohibits BLS employees and contractors who have access to prerelease CPI data from buying or selling Consumer Price Index futures. This prohibition is not currently relevant because CPI futures are not traded, but is still in effect.

We noted CPI staff is periodically provided updated data security procedures. CPI employees must sign a memorandum indicating that they fully understand the procedures and agree to adhere to them. Although the procedures do not specifically address ethics issues, they do provide that employees must not discuss embargoed data with anyone prior to release. Such a medium acts as a means of periodically reminding employees of their data security and ethics responsibilities.

A draft BLS position paper, dated March 26, 1997, made a recommendation BLS should, at a minimum provide its employees guidance stating that engaging in certain types of financial transactions with prerelease knowledge may violate standards for ethical conduct. To date, this guidance has not been issued.

BLS responded to our Statement of Facts as follows:

> *We are currently developing advisory employee guidance reiterating existing OGE restrictions and providing advice on avoiding a real or apparent conflicts-of-interest.*

Recommendations

To ensure employees who handle embargoed data are aware of ethics requirements and investment restrictions, we recommend the Commissioner:

1. Provide periodic ethics training to all employees who handle embargoed data.

2. Finalize the advisory guidance regarding investment practices.

3. Establish a means of ensuring that all employees are periodically reminded of their responsibilities regarding ethical conduct and investment practices.

BLS Response to the Draft Report

BLS responded that they will establish an ongoing training/awareness program for all employee and contractor personnel. It will include information on security, confidentiality, and ethical conduct/investment practices. This program should be developed by January 2000. It initially will be provided to all current personnel, and then will be available to new personnel on a continuing basis. The program will include periodic refresher training.

A BLS Commissioner's Order on investment practices was drafted in May 1999 and is being reviewed within BLS. The final directive should be issued by September 1999.

OIG Conclusion

Based on BLS' response to our Statement of Facts and draft audit report, OIG considers the above recommendations to be resolved. The recommendations can be closed when BLS provides adequate documentation that the corrective action has been implemented.

3. BLS Management Control Plan Was Incomplete

The BLS management control plan as currently designed meets the basic requirements set forth in OMB Circular A-123. In recent years, BLS has revised its management control plan to streamline the process and integrate statutory review requirements. However, we noted the required OMB Circular A-130 triennial reviews had not been performed for all computer applications. Furthermore, follow-up on corrective action for control deficiencies needed to be improved. As a result, the BLS management control plan may not fully achieve its objective to continuously monitor and improve the effectiveness of the agency's management controls.

Over the past few years, BLS revised its management control plan to identify six basic areas critical to BLS mission and function. These are: (1) program management; (2) financial management; (3) information technology; (4) personnel security; (5) physical security; and (6) data confidentiality. Also, starting in April 1998, BLS implemented what is referred to as the Quarterly Review and Analysis. This process is designed to involve management in assessing critical BLS areas. Each BLS program reports quarterly on its critical areas to a coordinating office which produces a summary report. Included in this report is status information on issues identified in previous periods. This is followed by a meeting with the Commissioner, the office chief, and other BLS officials.

Even though the BLS management control plan as currently designed meets the basic OMB Circular A-123 requirements, the following conditions need to be addressed.

a. Triennial OMB Circular A-130 Reviews Had Not Been Performed

BLS has not met the OMB Circular A-130 requirement that security reviews should be conducted every 3 years. Since 1991, BLS has performed only one series of OMB Circular A-130 security reviews of its major systems and installations. A BLS official told us that, in the early 1990s, the decision was made to postpone the OMB Circular A-130 reviews because of budget constraints. As a result, the security of BLS information systems is at a greater risk of loss and unauthorized access.

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires each agency to perform an independent review of security in each major application and installation at least every 3 years. For some systems with changing technology or systems undergoing major modifications, reviews may be required earlier than 3 years.

Furthermore, OMB Circular A-130, Section 8.a.9., requires that BLS, as a policy for safeguarding electronic information:

> *. . . ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information.*

We found OMB Circular A-130 reviews were not performed triennially prior to FY 1998. In fact, a DOL study in 1992 had noted BLS was overdue for application security reviews and recommended that they be expedited. The first series of OMB Circular A-130 reviews began in 1987 and three reviews were performed. The OMB Circular A-130 reviews were suspended and deferred due to their high cost and BLS budget limitations. During the suspension, BLS performed ad hoc internal security reviews. Starting in FY 1998, BLS management instituted OMB Circular A-123/A-130 Triennial Review Plan (TRP) which combined an installation review with a system review. The TRP covered one-third of the major programs each year. Three major programs were evaluated in FY 1998.

We evaluated the TRP and found planned review dates for major BLS programs. However, the TRP also showed that some major installations have not been scheduled for risk analysis or audits. For example, the TRP shows the LABSTAT and other installations have an "undetermined" review date. Additionally, BLS designed the TRP to incorporate installation reviews into the system reviews. BLS management control officials told us the combined reviews produced unsatisfactory results. Specifically, the CES and PPI survey offices which were involved in the two recent prerelease incidents had a review conducted shortly before the incidents occurred. However, the vulnerabilities that caused the incidents were not identified. As a result, BLS has placed the triennial reviews on hold pending the outcomes of current OIG and internal reviews. We agree with BLS this combined review approach may not be effective and needs to be reevaluated.

b. BLS Management Control Needs to Strengthen its Oversight for Corrective Action

To verify corrective action had taken place for audits and internal reviews, BLS management control staff depended on written responses from program management to determine if the recommendations were implemented. Although the responses adequately addressed the corrective actions taken, management control officials did not routinely verify corrective action had been implemented and was operating as designed. As a result, corrective action may not have been implemented or may not have been sufficient to correct the identified control weakness.

According to OMB Circular A-123, *Management Accountability and Control*, responsibility for correcting deficiencies rests with agency management. The Circular states:

> . . . *a determination that a deficiency has been corrected should be made only when sufficient corrective actions have been taken and the desired results achieved.*

The management control staff relied strictly on written reports as notice that corrective action had been implemented. As a result, audits and internal reviews continued to identify similar problems. For example, our review of the January 1999 prerelease incident found problems similar to ones identified in an internal 1996 review.

Following a prerelease of PPI data in 1996, the management control staff performed an internal review and made six recommendations. Program management responded to each of the six recommendations with a corrective action plan. Two years later in November 1998 program management provided an update to the six recommendations. The update contained sufficient detail on the corrective actions taken and confirmed that changes had been made and were complete. However, we found that the corrective action taken failed to correct the identified problems and subsequent reviews identified similar problems. BLS management control staff agreed that verification of the improvements made since 1996 may have prevented the recurrence of problems. The BLS management control staff told us they are currently considering what verification efforts should be included in following up on correcting high risk internal control deficiencies.

Three additional examples in which problems found during our audit were similar to problems disclosed in previous reviews follow:

(1) A 1989 OIG audit of the BLS LAN reported that physical access to servers can be improved and LAN password policies and procedures need to comply with FIPS.

(2) A 1991 contractor security review of PPI reported work areas were open during the workday, software changes were not done in a controlled environment to ensure that the changes were authorized and adequately tested before being moved to production, appropriate segregation of duties did not exist in that applications programming and systems programming had write access to PPI production data, not all employees and contractors who had access to embargoed data had background investigations, and sensitive computer printouts from the remote printer room were delivered to a table in an open unsecured area with no required verification that the correct number of copies were received.

(3) A 1992 DOL Solicitor review of BLS-ETA data security noted that OMB Circular A-130 reviews could be viewed as overdue because BLS programs had not been reviewed since 1989. The Solicitor recommended that BLS expedite its application security reviews.

BLS responded to our Statement of Facts as follows:

> *The BLS had performed formal A-130 reviews for approximately five years before suspending the formal program in 1991. Other*

> *internal security reviews were conducted on some programs as described in the audit observations. In 1998, BLS developed and reinstituted an A-123 and A-130 triennial review plan for our major programs. Three programs (PPI and the CPS and CES components of the Employment Situation) were reviewed by a contractor in FY 1998. The BLS plans to continue these reviews and will re-assess its plans following the completion of the current OIG and internal security audit/review activities.*

Recommendations

To improve the BLS management control process, we recommend the Commissioner:

1. Revise and finalize the Triennial Review Plan to ensure all major systems are reviewed every 3 years.
2. Ensure adequate funding is provided to review all major systems at least every 3 years.
3. Discontinue the approach of incorporating the installation reviews into system reviews for high-risk areas.
4. Develop and implement follow-up procedures that require management control staff to verify the effectiveness of the corrective action taken by management on high-risk internal control deficiencies.

BLS Response to the Draft Report

BLS responded that a proposed triennial A-123/130 review plan has been prepared for consideration by the Data Security Steering Committee. The plan covers the BLS Principal Federal Economic Indicators, selected additional systems, and IT installations (a total of 12 components). The plan should be finalized in July 1999 and BLS will ensure that ongoing funding is allocated to accomplish the triennial review plan. Additionally, the proposed triennial review plan provides for a separate review of each major BLS installation: the mainframe computing center, the BLS LAN/WAN, and the BLS public web site.

Concerning follow-up procedures, BLS responded that additional staffing and resources will be allocated to the BLS Management Control Program, and recommendation follow-up policies and procedures will be established to permit verification of corrective actions on high-risk internal control deficiencies. These staff, resources, policies, and procedures should be fully in place by July 2000. In the interim, current management control staff will take steps to develop and implement an effective verification follow-up process.

OIG Conclusion

Based on BLS' response to our Statement of Facts and draft audit report, OIG considers the above recommendations to be resolved. The recommendations can be closed when BLS provides adequate documentation that the corrective action has been implemented.

BLS INITIATIVES

Since the two recent prereleases, the intrusion into the BLS web page, and OIG's audit, BLS has taken actions and implemented initiatives to prevent further incidents.

The first prerelease incident occurred on Thursday, November 5, 1998, for the October 1998 Employment Situation Report news release. The incident involved the posting of supplemental news release tables to the BLS web site. As a result of the prerelease, the Commissioner directed an internal review be conducted of the incident and the results reported to her. The report was completed on November 19, 1998, and a copy was provided to the Secretary of Labor and the Inspector General. The Commissioner also directed BLS: (1) cease posting supplemental tables to the BLS web site until procedural safeguards could be reviewed and strengthened; and (2) review every process connected with posting data to the BLS web site. The Commissioner requested the Inspector General to assist BLS in a comprehensive audit of all activities associated with the dissemination of sensitive economic data.

On January 12, 1999, BLS experienced another prerelease. This prerelease involved PPI data. On January 14, 1999, BLS and OIG initiated a joint review to identify the processes/causes involved. The Commissioner provided a report to the Secretary of Labor and Inspector General on the results of the review on January 25. The Commissioner directed interim procedures be implemented to limit the amount of time files are available on the internal servers prior to the official release time. The Commissioner also held security sessions with all BLS managers. She instructed them to reiterate data security policies to their staff**.**

On February 22, 1999, the Commissioner instructed the Associate Commissioners to create an inventory of all data releases, the methods of dissemination and document the procedures for each news release. They were to review, reassess, improve and document their internal procedures. The Commissioner established a steering committee headed by the Deputy Commissioner to facilitate this effort. A separate team has been established to review the processes, with the first phase focusing on the security of embargoed data. During our field work, we found some of the survey offices had already begun this process.

In April 1999, BLS formed the Configuration Management Team to produce a series of guidelines which will include IT concepts such as version control, independent process review and change control. On April 6, 1999, BLS Office of Administration published a draft Personnel Security Review report. The review is part of an overall evaluation of BLS activities associated with the dissemination of sensitive economic data. Additionally, in April 1999 the BLS Data Security Review Team completed a physical security review of the Postal Square Building.

Exhibit I

EXHIBIT I - BLS COMPLETE RESPONSE TO THE DRAFT REPORT

Attachement

Bureau of Labor Statistics (BLS) Response to Office of Inspector General (OIG) Draft Audit Report No. 09-99-007-11-001

Note: Recommendations were not numbered in the OIG report. In this response, recommendations are numbered based on their location in the report as follows: the first digit is the chapter number, the second digit is the section number, and the third digit is the sequence number in which the recommendation was listed within the section.

1.1.1. Establish controls to ensure all available web security features are enabled.

The BLS has implemented this recommendation.

New web software (Microsoft Internet Information Server 4.0) has been installed and comprehensively configured. As part of this installation process, security scripts were run to test for the presence of recommended patches. Microsoft and other security-related news services are being monitored by the LABSTAT system administration staff, in conjunction with LAN Support staff and the BLS security team to keep appropriate personnel informed of threats and appropriate countermeasures.

1.1.2 Act on all findings in the NSA Security Report.

Implementation of this recommendation is underway and should be completed, to the extent possible, by November 1999. To date (as of June 11, 1999), BLS has made changes to implement 37 of NSA's 82 recommendations.

As indicated in the NSA report, BLS may not be able to implement all of NSA's recommendations without making some of the BLS web site unavailable to the public. Public access is the primary purpose of the web site. The NSA report stated that the recommendations were made "only to assist you in choosing the correct posture in which to operate at 100% efficiency … it is possible that certain operational commitments will not be met if all the recommendations are implemented." This indeed is the case. BLS is preparing an evaluation of the impact of implementing each of NSA's recommendations and will meet with the OIG to review the results of this evaluation.

1.1.3 Require LABSTAT to obtain and implement a standard library management system to protect software.

Implementation of this recommendation is underway and should be completed by August 1999. LABSTAT has implemented Microsoft Visual Source Safe version control software. At present all data loading scripts have been entered into the Source Safe library management system; all other LABSTAT source code is currently being entered.

1.1.4. Develop policies and procedures for LABSTAT which provide for controls over changes, upgrades, testing and implementation of both system and application software.

Implementation of this recommendation is underway and should be completed by January 2000. The general policies have been set. Version control software is in place. More specific procedures will be developed and implemented when a new staff member is hired to take the role of librarian and configuration management coordinator.

1.1.5. Require the independent review/quality assurance function be performed for all modifications before placing programs or systems into production.

Implementation of this recommendation is underway and should be completed by November 1999. LABSTAT established a new independent Quality Control team in February 1999. It is headed by one long-time LABSTAT procedures member, and currently is staffed by two contractors. LABSTAT is recruiting for three new federal employees to replace the two contractors, bringing the team to a total strength of four people.

The team has developed comprehensive test plans for the two central LABSTAT production scripts – News Releases and Time Series updates – and has performed two rounds of independent testing, one in February for the introduction of new Sun hardware, and one in May for the roll-out of the Spring 1999 version of the LABSTAT system. The team next will develop quality control/test plans and procedures for system level changes (in addition to the test plans already developed for the production scripts).

1.1.6. Restrict access to all [LABSTAT] programming source code.

The BLS has implemented this recommendation. File permissions currently are set so that only the LABSTAT Data Management branch chief has write access to the data loading scripts on the production machines. Such access restrictions are likely to become more sophisticated once the configuration management coordinator is on board.

1.1.7 Ensure LABSTAT develops formal documentation outlining duties, responsibilities and lines of communication.

Implementation of this recommendation is underway and should be completed by January 2000.

LABSTAT management is working on a comprehensive reorganization plan, which includes considerable information on duties, responsibilities, and lines of communication. This reorganization plan has been approved by BLS management. The reorganization plan documents will be supplemented by operational documentation containing additional details on duties, responsibilities, and lines of communication.

1.1.8. Ensure staff outside of LABSTAT is not allowed to post information to the web site.

The BLS has implemented this recommendation. File permissions on the LABSTAT production machines, both inside and outside the firewall, are set so that only LABSTAT staff may write to these machines.

1.2.1. Ensure procedures are developed to periodically review and test access controls at SunGard to ensure BLS data is secure.

Implementation of this recommendation is underway and should be completed by October 1999. The BLS Information Technology (IT) Security Team has been assigned the responsibility for testing IT security controls at SunGard. They will develop/acquire tools and establish procedures for regularly testing file and tape access controls at SunGard.

1.3.1. Require the independent review/quality assurance function be performed for all modifications before placing programs or systems into production.

Implementation of this recommendation is underway and should be completed in July 1999. Independent review/quality assurance will be required for all modifications before placing any programs or system into production. The BLS Office of Technology and Survey Processing (OTSP) approved procedures on May 10, pending certain minor changes, which require acceptance testing that is independent of the developer(s) who made the modifications.

1.3.2. Obtain and implement a standard library management system to protect software.

Implementation of this recommendation is underway and deployment should begin by January 2000. OTSP has chartered a team to identify an appropriate standard library management system or systems. It is likely that there will be more than one such system – OTSP does not expect that a single system will be appropriate for both the mainframe and the LAN/personal computer environments. The team should make its recommendations by October 1999, and management will act on the recommendations expeditiously. In cases where a mainframe system is in the process of being downsized to the LAN environment, the library management system generally will be deployed in the downsized environment. We will ensure that interim safeguards are in place as appropriate.

1.3.3. Restrict access to all programming source code.

Implementation of this recommendation is underway and should be completed in July 1999. Substantial restrictions to programming source code have long been in place. Additional restrictions were included in the new configuration management processes adopted by OTSP on May 10, pending certain minor modifications. (See BLS response to recommendation 1.3.1.) These restrictions authorize only system librarians to move source code to and from production libraries.

1.4.1. Test the continuity of operations in all BLS mission critical systems.

Implementation of this recommendation is underway. Continuity of Operations Plans (COOPs) for all mission-critical systems should be developed by January 2000, and testing of critical systems that produce a Principal Federal Economic Indicator should be completed by January 2002.

The costs and staff time involved in testing a COOP prohibit the BLS from quickly testing all plans in a short time frame. The BLS plans to test one COOP before the end of Calendar Year 1999. Based on the information gathered from that test, a schedule will be developed for testing the COOPs of all other mission critical systems; at a minimum, testing for each Principal Federal Economic Indicator system should be completed by January 2002, and testing for LABSTAT should be completed by June 2002. In the interim, portions of each system’s COOPs will be tested in order to verify server and application recovery procedures.

1.4.2. Update and periodically review the BLS IT security plan.

Implementation of this recommendation is underway and should be completed by January 2000.
The intent of the BLS IT Security Plan is to document mitigating security controls within the environment; it is not intended to identify and assess the impact of vulnerabilities. The identification and impact of vulnerabilities should be completed during a risk analysis process. The BLS has not completed a recent risk analysis. A risk analysis should be completed by the end of Calendar Year 1999, and BLS will update the IT Security Manual as appropriate. Additionally, the BLS is updating its triennial A-123/130 review plan. It will cover the BLS Principal Federal Economic Indicators, selected additional systems, and IT installations. The updated A-123/130 review plan should be finalized in July 1999.

1.4.3. Require each server administrator to periodically test and ensure technical security controls are adequate.

Implementation of this recommendation is underway and should be completed by October 1999.

The BLS will institute a quarterly certification process, which will require server administrators to complete a security checklist and submit it to the IT Security Team for review. The IT Security Team will continue and expand the content of its current monthly audits of all BLS servers.

1.4.4. Develop and implement IT security procedures to require all servers and backup media be located in a secure location with limited access.

OTSP has chartered a team to review the physical location and logical administration of all servers within the BLS. This team will produce recommendations on the following:

- Physical security requirements for areas housing servers.
- Relocation of existing servers.
- Future location of new servers.
- Responsibility for server administration of existing servers.
- Assignment of server administration for new servers.
- Centralization of specific administrative tasks.

Following completion of the team's work, the BLS will make and implement decisions on the physical location(s) and security of servers and backup media.

1.4.5. Require each survey office to establish a position for a qualified individual to be responsible for security oversight of all its servers.

The OTSP team described in the BLS response to recommendation 1.4.4 will make recommendation(s) to ensure that individuals assigned the responsibility for server administration and security receive adequate training to fulfill that responsibility. Full implementation of this recommendation should be completed by July 2000. In the interim, OTSP will strengthen its current server oversight activities (for example, increased auditing) to protect the security of data stored on BLS servers.

1.4.6. Strengthen controls over data lines by implementing procedures to require all requests for data lines be justified and be reviewed by the IT security team.

The BLS has implemented this recommendation for National Office data lines, and a procedure to ensure appropriate clearance of requests in the regional offices should be in place by September 1999. All National Office requests for data lines now must be approved by the IT Security Team before the lines are provided.

1.4.7. Identify and review all existing data lines to ensure they are needed.

The BLS has implemented this recommendation for National Office data lines, and implementation in the regional offices should be completed by October 1999. An inventory of data lines in the National Office was completed in June 1999, and data lines identified as unused were eliminated. An inventory of data lines in the regional offices is being initiated, and any unused regional data lines will be identified and eliminated.

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.

The BLS has partially implemented this recommendation and should complete all aspects of implementation by October 1999, as follows:

- Deletion of Separated Users' Accounts – BLS Information Technology security policy 3.1.19 addresses this requirement. The BLS will develop an effective separations process for both employees and contractors, and will issue separations checklists to all supervisors. Network and subnetwork administrators will be informed of BLS employee and contractor separations. On or before midnight of the day following the user's last day of work, network or subnetwork administrators will disable, delete, or change the password for accounts used by the separated employee or contractor. Unless otherwise instructed by the separated person's manager, the default action will be to change the account password. If the account is disabled or the password is changed, the administrator will delete the account within 20 business days of the user's last day of work. This procedure should be fully in place for all personnel and all types of accounts by October 1999.

- Deletion of Inactive Accounts – On the first business day of each month, network and subnetwork administrators will check for accounts that have not been accessed within the last 30 days. When such an account is encountered, an E-mail message will be sent to the account owner's manager to determine if the account is still valid. If a response is received that the account is still valid, no action will be taken; otherwise the account will be disabled, and then deleted within 20 business days. The procedure for identifying inactive NT accounts should be in place in July 1999. The procedure for identifying inactive UNIX accounts is being developed and should be implemented by October 1999.

- Management Review of Accounts – Managers will be required to verify computer accounts annually. On the first business day in October, network and subnetwork administrators will produce a list of all user accounts defined on their systems. The administrators will parse this list by division or office; accounts that cannot be classified to a particular division or office will be included under a section labeled *Other*. The administrators will send a listing of the user accounts identified in an office or division to the appropriate manager along with a listing of the accounts identified as *Other*. It is the responsibility of the manager to have these accounts reviewed and to identify those accounts that should remain active. Any account not identified as active by the last business day in October will be disabled and subsequently deleted within 20 business days. The procedure for this annual management review of NT and UNIX accounts should be in place in July 1999.

1.4.9. Improve IT security by installing software to encrypt passwords on servers where the passwords are stored and before one-way transmission from point-of-entry to point-of-authentication.

An evaluation is underway to determine whether BLS can fully implement this recommendation, and implementation should be completed as fully as possible by July 2000.

1.4.10. Encrypt confidential and embargoed files wherever possible.

Work is underway to determine the extent to which BLS can encrypt confidential and embargoed files, and expanded use of encrypted files should be implemented by July 2000.

1.4.11. Require password changes every 30 days.

The BLS plans to change its password policy to require that passwords be changed every 90 days instead of every 180 days. The NSA report recommended that BLS policy be established to require changing passwords every 90 days; and 90 days is within the range of GAO's guidelines. BLS believes that requiring users to change passwords every 30 days would lead to an increased security vulnerability because users would be more likely to write their passwords down in order to remember them. The planned change in password policy should be implemented by October 1999.

1.4.12. Require screen saver password protection for all workstations.

The BLS has implemented this recommendation. The BLS has established an official policy requiring that password protected screen savers be enabled on all workstations and servers and that a maximum inactivity time of 15 minutes be used. This policy has been announced to all employees and contractors and installation instructions have been made available. Automated methods for auditing and enforcement are being developed.

2.1.1. Develop BLS-wide security standards to be followed by survey offices.

The BLS will issue a Commissioner's Order on management control and data security and an Administrative Procedure on data security standards. These directives should be issued by October 1999.

2.1.2. Ensure comprehensive policies and procedures manuals are developed for preparation and dissemination of sensitive news releases.

The BLS has implemented this recommendation. In February 1999, a BLS Data Security Steering Committee and Data Security Review Team were formed. The team is conducting a thorough review of the security of sensitive news releases. The Commissioner directed the statistical program offices to document all processes for preparing and disseminating embargoed data, with the involvement of the supporting OTSP project offices. Other offices involved in data dissemination also documented their processes. These offices submitted their documentation to the Security Review Team, and the team analyzed the documentation for adherence to key security principles. Offices will be directed to make any necessary improvements to their documentation based on the team's feedback and to incorporate new BLS security standards that are being developed.

2.2.1. Ensure work areas for preparation of news releases are segregated and secure.

The BLS is in the process of implementing this recommendation. The BLS Security Review Team has addressed the physical security of sensitive news releases, and the Steering Committee has approved a number of team recommendations. All BLS Principal Federal Economic Indicators now will be released through the Department of Labor "lock-up" procedure. Advance copies of these releases will be printed in the Postal Square Building rather than at the Department of Labor Print Shop. Physical access to areas where these data are present will be restricted to authorized individuals, and "restricted access" signs will be placed at entrances to those areas. These actions should be completed by November 1999.

Over the long term, the BLS will consider the advisability and feasibility of reconfiguring office space to segregate staff who work on these releases. We may conclude, however, that alternative measures can be used to achieve the appropriate level of security.

2.3.1. Strengthen and enforce policies and procedures for safeguarding printouts with confidential and embargoed data.

The BLS is taking a number of actions to implement this recommendation. The Office of Administration is preparing a memorandum to all BLS personnel on this matter. It will remind them that confidential printed material (material displaying respondent-identifying or pre-release data) must be treated in a secure manner in accordance with BLS Administrative Procedure 1-96. It will instruct them to avoid excessive printing of listings containing confidential material, and will inform them of the facilities available for the authorized disposal of printed confidential material. This memorandum will be issued in July 1999.

Triennial application security reviews of BLS programs will include an assessment of whether confidential printed material is being treated in a secure manner.

Enhanced physical controls over entry points to the ground floor computer center will be installed by January 2000. Confidential material is not printed on the central LAN printers in room 2810 of the Postal Square Building. As a precautionary measure, however, a sign stating that the central LAN printers should not be used for printing sensitive or embargoed data has been posted in the print job pick-up area in room 2810.

2.4.1. Strengthen and enforce policies and procedures for protecting electronic files containing sensitive data.

The BLS has implemented or is implementing several OIG recommendations that will strengthen and enforce policies and procedures for protecting electronic files containing sensitive data. Examples most directly related to this recommendation are the BLS actions in response to recommendations 1.1.2 (acting on NSA findings); 1.2.1 (SunGard access controls); 1.4.3, 1.4.4, and 1.4.5 (server and backup media security); 1.4.8 (computer account management; and 1.4.11 and 1.4.12 (passwords and password-protected screen savers).

The BLS has discontinued the storage of sensitive data on computer C-drives, with the exception of a secure procedure where the computer is stored in a locked room used by authorized persons exclusively for preparing sensitive news releases. The storage of sensitive data on diskettes is being re-evaluated on a case-by-case basis and discontinued where appropriate. Any diskettes containing sensitive material will be handled in a secure manner and stored in locked receptacles.

2.5.1. Establish flexiplace policies and procedures which address data security requirements.

The BLS has drafted proposed flexiplace policies and procedures addressing data security requirements, and they currently are being evaluated by senior management. Final policies and procedures should be issued by September 1999.

3.1.1. Ensure the sensitivity level for all positions is accurately classified.

The BLS will conduct a thorough review of all employee and contractor positions and will update position risk designations in accordance with the latest OPM guidance. Then, based on the position risk designations, BLS will initiate appropriate security checks/clearances (NACI at a minimum) for all employee and contractor personnel as necessary. Procedures will be put in place to ensure that appropriate security checks/clearances are performed on all new employee and contractor personnel, and on personnel who change positions within the BLS. All of these actions should be completed for personnel who work with pre-release data for the Principal Federal Economic Indicators by January 2000, and for all other personnel by April 2000.

3.1.2. Ensure appropriate security clearances are obtained for all employees in critical or sensitive positions.

Please see the BLS response to recommendation 3.1.1.

3.1.3. Ensure NACI checks are performed for all contract staff and appropriate security clearances are obtained for all contract staff performing critical or sensitive duties.

Please see the BLS response to recommendation 3.1.1.

3.1.4. Ensure procedures are instituted to continually monitor the sensitivity of position classifications and employee and contractor security clearances.

Please see the BLS response to recommendation 3.1.1.

3.2.1. Provide periodic ethics training to all employees who handle embargoed data.

The BLS will establish an ongoing training/awareness program for all employee and contractor personnel. It will include information on security, confidentiality, and ethical conduct/investment practices. This program should be developed by January 2000. It initially will be provided to all current personnel, and then will be available to new personnel on a continuing basis. The program will include periodic refresher training.

3.2.2. Finalize the advisory guidance regarding investment practices.

A BLS Commissioner’s Order on investment practices was drafted in May 1999 and is being reviewed within BLS. The final directive should be issued by September 1999.

3.2.3. Establish a means of ensuring that all employees are periodically reminded of their responsibilities regarding ethical conduct and investment practices.

Please see the BLS response to recommendation 3.2.1.

3.3.1. Revise and finalize the Triennial Review Plan to ensure all major systems are reviewed every 3 years.

A proposed triennial A-123/130 review plan has been prepared for consideration by the Data Security Steering Committee. The plan covers the BLS Principal Federal Economic Indicators, selected additional systems, and IT installations (a total of 12 components). The plan should be finalized in July 1999.

3.3.2. Ensure adequate funding is provided to review all major systems at least every 3 years.

The BLS will ensure that ongoing funding is allocated to accomplish the triennial review plan.

3.3.3. Discontinue the approach of incorporating the installation reviews into system reviews for high-risk areas.

The proposed triennial review plan provides for a separate review of each major BLS installation: the mainframe computing center, the BLS LAN/WAN, and the BLS public web site.

3.3.4. Develop and implement follow-up procedures that require management control staff to verify the effectiveness of the corrective action taken by management on high-risk internal control deficiencies.

Additional staffing and resources will be allocated to the BLS Management Control Program, and recommendation follow-up policies and procedures will be established to permit verification of corrective actions on high-risk internal control deficiencies. These staff, resources, policies, and procedures should be fully in place by July 2000. In the interim, current management control staff will take steps to develop and implement an effective verification follow-up process.