

U.S. DEPARTMENT OF COMMERCE
Office of Inspector General



ECONOMICS AND STATISTICS
ADMINISTRATION

Additional Security Measures Needed for
Advance Retail Sales Economic Indicator

Final Inspection Report No. OSE-12754/September 2001

PUBLIC
RELEASE

Office of Systems Evaluations

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
INTRODUCTION	1
BACKGROUND	2
OBJECTIVES, SCOPE, AND METHODOLOGY	7
FINDINGS AND RECOMMENDATIONS	9
I. Application Controls Should Be Strengthened	9
A. Physical access controls for servers on the LAN are reasonable, but guidance for personnel access to branch spaces needs improvement	9
B. Logical access controls are appropriate	11
C. Application software change control is informal and lacks documented procedures	12
D. Auditing software has not been regularly used during lockup	13
E. Recommendations	13
II. Management Controls Over Personnel Security Need to Be Strengthened	15
A. Employees have not had appropriate background investigations	18
B. Risk levels for positions have not been properly assigned	19
C. Guidance concerning legal and ethical restrictions on investments based on advance knowledge is not adequate	19
D. Recommendations	20
APPENDIXES	
A. Purpose and Critical Elements of Major Categories of FISCAM General Controls	
B. BLS Commissioner's Order No. 1-00	
ATTACHMENT	
A. ESA's and Census Bureau's Response to Draft Inspection Report (excluding attachments to the response)	

EXECUTIVE SUMMARY

Two bureaus within the Economics and Statistics Administration, the Census Bureau and the Bureau of Economic Analysis, develop Principal Federal Economic Indicators, which are major statistical series that describe the current condition of the nation's economy. Because these indicators have significant commercial value, may affect the movement of commodity and financial markets, and may be taken as a measure of the impact of government policies, no information associated with them should be disclosed before their official release time. Many indicators are based on confidential data voluntarily provided by businesses, which also must be protected. Thus, maintaining the security of the indicators throughout the preparation and release process is of utmost importance.

This report presents the results of our evaluation of the security of the Census Bureau's Advance Retail Sales Principal Federal Economic Indicator. The bureau's indicators are the responsibility of the Associate Director for Economic Programs. We selected this indicator for evaluation because of its high degree of importance and sensitivity.

When initial estimates of the Advance Retail Sales indicator become available, bureau staff operate in a "lockup," or secure, mode in order to safeguard the estimates, which are refined over a period of several days. ESA is responsible for releasing the indicators to the public. It provides the indicator information to reporters from various news organizations 30 minutes before the official release time in a secure press room (lockup facility) and allows the reporters to prepare stories that are transmitted to their news organizations at the official release time. After its official release, the information is also made available to the public on the ESA and Census Bureau web sites.

The objective of our evaluation was to determine whether ESA and the Census Bureau have adequate internal controls to prevent the premature or unauthorized disclosure or use of Advance Retail Sales economic indicator data before it is released to the public. We evaluated the effectiveness of (1) application controls associated with information technology resources used to prepare the indicator and (2) management controls over personnel security for Census Bureau and ESA staff having advance knowledge of the indicator.

The bureau's access controls appropriately establish individual accountability and limit the processing privileges of individuals. In addition, physical access controls for servers used to develop the indicator are reasonable. However, other aspects of application controls should be strengthened, and management controls over personnel security need to be improved:

- **Guidance for personnel access to branch spaces needs improvement.** The procedures for access to branch spaces during lockup do not state explicitly that branch members are required to use only the designated controlled access door or address measures to protect information when personnel who are not authorized access to sensitive data require

admittance to branch spaces. We recommend that the procedures be modified to address these omissions. (See page 9.)

- **Application software change control is informal and lacks documented procedures.** Although a process is in place for requesting changes to the application software, there are no written procedures for making the changes and performing and documenting appropriate tests on the modified software to ensure that only authorized changes are made. We recommend that procedures for software change control be developed in accordance with bureau and Department guidance. (See page 12.)
- **Auditing software has not been regularly used during lockup.** When audit logs were available, they were not used regularly to monitor access to the indicator data. As a result of a recent upgrade to the operating system of the server where the indicator data is stored, the audit logs cannot be provided in the format required by the audit application program, so these logs will not be available until this program is replaced. We recommend that a commercially available audit application be selected and installed as soon as possible and that written procedures and training on its use be provided. (See page 13.)
- **Employees have not had appropriate background investigations, and risk levels have not been properly assigned.** Only one of three employees associated with Advance Retail Sales in positions classified as moderate risk have undergone the appropriate background investigation required by the Office of Personnel Management (OPM); the other two have undergone less intensive investigations. The Office of Security could not identify the type of investigation done, if any, for the majority of the positions classified as low risk in another division of the Economic Directorate. Two persons designated as alternate ESA press room lockup directors also have not undergone appropriate background investigations. Furthermore, risk levels assigned to some positions are inconsistent with their levels of responsibility and trust. We recommend that appropriate background investigations be completed for all employees having pre-release knowledge of economic indicator data and that position sensitivity classifications be reassessed to ensure that they reflect the appropriate level of responsibility and trust in accordance with OPM guidance. (See page 18.)
- **Guidance concerning legal and ethical restrictions on market investments based on advance knowledge is not adequate.** Census Bureau and ESA employees who have access to pre-release indicator data are not provided written guidance regarding the legal and ethical restrictions on investing in financial markets based on advance information. We recommend that specific guidance be provided on how the Standards of Ethical Conduct for Employees in the Executive Branch restrict employees' ability to engage in certain financial transactions with knowledge of pre-release economic indicator data. (See page 19.)

In our efforts to identify the criteria that are used to determine appropriate risk levels and their associated background investigations, we noted a lack of guidance from the Department's Office of Human Resources Management and the Office of Security, suggesting that the issue of appropriate risk levels and background investigations may exist elsewhere in Commerce. We have addressed this issue in our report, *Program for Designating Positions According to Their Risk and Sensitivity Needs to Be Updated and Strengthened*, Draft Inspection Report No. OSE-14486/August 2001, which includes recommendations for the Department to provide to operating units updated guidance for determining appropriate risk levels and their associated background investigations.



ESA and the Census Bureau have agreed with and are taking steps to implement all of our recommendations. Our recommendations, which begin on page 13 and page 20, include a synopsis of their response and our comments on the response, where appropriate.

In particular, the bureau has indicated that positions held by all personnel working on indicator surveys would be designated as moderate risk, based on discussions with the OIG. However, our intent was not to specify a particular designation, but rather to point out that designations should be based on the level of the position's responsibility and trust in accordance with guidance from the bureau's Human Resources Division.

Since we completed our work on the Advance Retail Sales indicator, the Department's Office of Security and Office of Human Resources Management have agreed to provide to operating units updated guidance for determining appropriate risk levels and their associated background investigations. Therefore, the bureau's Human Resources Division needs to ensure that its efforts to implement our recommendations are consistent with the Department's forthcoming guidance.

The response of ESA and the Census Bureau, excluding its attachments, is included as Attachment A.

INTRODUCTION

This report presents the results of our evaluation of the security of the Census Bureau's Advance Retail Sales Principal Federal Economic Indicator, one of the major statistical series that describe the current condition of the economy of the United States. Principal Federal Economic Indicators are developed not only by the Department of Commerce, but also by the Departments of Agriculture, Labor, and the Treasury, and the Federal Reserve Board, and include the Gross Domestic Product, U.S. International Trade in Goods and Services, Farm Sector Income, Unemployment Rate, Consumer Price Index, World Agricultural Production, and Consumer Installment Credit.

These indicators are widely watched and heavily relied upon by government and the private sector for an understanding of the current condition and future direction of the nation's economy. They have significant commercial value, may affect the movement of commodity and financial markets, and may be taken as a measure of the impact of government policies. The indicators are compiled, released, and periodically evaluated by the various agencies in accordance with Office of Management and Budget (OMB) Statistical Policy Directive No. 3, which provides procedures to ensure that the indicators meet specific accuracy, release, and accountability standards.

Department of Commerce Principal Federal Economic Indicators

For the Department of Commerce, two bureaus within the Economics and Statistics Administration are responsible for developing Principal Federal Economic Indicators. The Bureau of Economic Analysis develops such indicators as the Gross Domestic Product, Corporate Profits, and Personal Income and Outlays indicators. The Bureau of the Census develops indicators that include Advance Retail Sales, Housing Starts and Building Permits, and Wholesale Trade.

In keeping with OMB's directive, ESA publishes a yearly schedule of the time and date that each of its indicators will be officially released to the public. ESA releases the indicators from a secure press room (referred to as the "lockup" facility). Security is needed because OMB's directive requires agencies to ensure that no information or data estimates associated with the indicators are disclosed before the official release time.

BACKGROUND

The Census Bureau's Associate Director for Economic Programs is responsible for developing the bureau's Principal Federal Economic Indicators. Within this directorate (referred to as the Economic Directorate), the Service Sector Statistics Division's Retail and Wholesale Indicators Branch develops the Advance Retail Sales indicator.

Advance Retail Sales Economic Indicator—General Background

The Advance Retail Sales indicator is released to the public in the Advance Monthly Retail Sales Report. This report contains the advance sales estimates for the reporting month and preliminary sales for the previous month by type of business, such as automotive dealers, furniture and home furnishings stores, food stores, eating and drinking places, and gasoline service stations. It includes both seasonally adjusted and unadjusted data and is typically released on the ninth business day of the month following the month to which the report applies. For example, the indicator for April is released on the ninth business day of May.

This indicator is widely used by government, academic, and business organizations. It is an input to developing the Gross Domestic Product, is used by the Council of Economic Advisors for economic policy analysis, and provides the Federal Reserve Board a basis for anticipating economic trends. For instance, lower-than-expected sales figures could be seen as an indication of a weakening economy and hence portend higher bond prices. The news media regularly report on this indicator and use the estimates for performing economic analyses. Businesses use the estimates to gauge how well they are performing and to predict future demand for their products, and financial analysts and market research organizations use the data to analyze market trends and forecast the direction of the economy.

Advance Retail Sales—Development Process

The timeline for development and release of the Advance Retail Sales indicator is presented in Figure 1. Data for developing the indicator is collected through the Advance Monthly Retail Sales Survey. Near the end of the month for which the indicator is to be developed, survey forms are either mailed or sent by facsimile to a sub-sample of about 4,100 participating businesses selected from the Monthly Retail Trade Survey sample of more than 12,000 businesses. Businesses participate on a voluntary basis and are afforded confidentiality by the bureau as required by Title 13 of the United States Code.

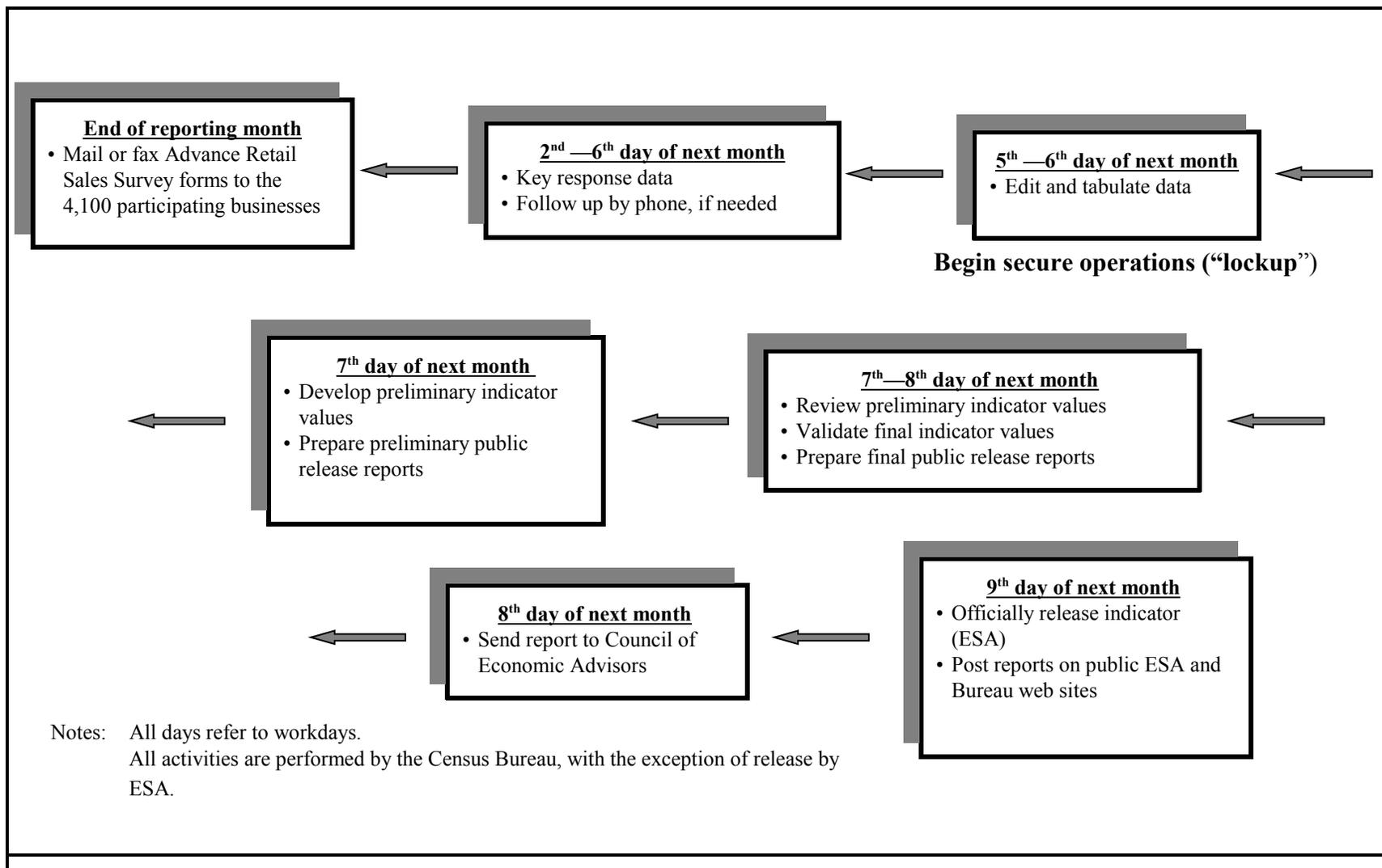


Figure 1. Timeline for Development and Release of Advance Retail Sales Indicator

Completed survey forms are returned either by mail or facsimile to the National Processing Center (NPC) in Jeffersonville, Indiana, where response data is keyed starting on the second workday of the following month. Data keying continues during the third through sixth workdays, when telephone follow-up is used to obtain information from those businesses whose responses were not provided via mail or facsimile, or included information that needed clarification.

Editing and tabulation of the survey data begin on the fifth workday, and at this point, initial estimates of the indicator values become available. Consequently, starting on the fifth workday and extending through the release on the ninth workday, the Retail and Wholesale Indicators Branch staff operates in a lockup, or secure, mode in order to safeguard the evolving estimates. During the morning of the seventh workday, branch staff develop finalized indicator values and prepare reports for public release. The finalized numbers are subject to change during the validation and review process performed by management and staff. The remainder of the seventh day and the eighth day are spent on validating the final values and preparing materials for public release. Late on the afternoon of the eighth day, the report is sent to the Council of Economic Advisors by secure facsimile.

At 7:45 a.m. on the ninth workday, managers from the Retail and Wholesale Indicators Branch deliver final distribution copies of the Advance Monthly Retail Sales Report and diskettes containing the report to the ESA lockup director or a designated alternate. At 8:00 a.m., in a locked office, the managers brief the Department's Under Secretary for Economic Affairs, Deputy Under Secretary for Economic Affairs, and Chief Economist. The office where the briefing is held remains locked until 8:30 a.m., the official release time. The information is officially released through the ESA press room, and the report is then made available to the public on the ESA and Census Bureau web sites.

Principal Economic Indicator Release Process

On the date that an indicator is scheduled for release, reporters from various authorized news services may enter the lockup facility, located at Department headquarters in Washington, D.C., one hour before the official release time. Until one half hour before release time, reporters may use their computer and communications equipment housed in the lockup facility or brought with them to establish communications with the external news service systems that will receive the indicator data. One half hour before release time, reporters are required to break off communications with their external systems. The door is locked, and nobody may enter or leave the facility until after official release of the indicator. The ESA lockup director distributes hardcopy reports and diskettes containing the indicator data to the reporters, who may ask questions about the information and prepare stories for transmission to their external systems. Communications are reestablished at the release time.

Incidents During the Release Process Have Prompted Tighter Controls by ESA

In February 2000, the New Home Sales indicator was released to one reporter's remote site nearly 30 minutes early, and in April 2000, a story on the Trade Deficit indicator for a different news service appeared on the service's web site with a time stamp three minutes earlier than the official release time. We assessed these incidents and found that the first release occurred because, until recently, communications were provided by individual electronic switches connected to the reporters' computers, which the reporters controlled themselves under the scrutiny of ESA personnel. In this instance, the communications line had been disconnected from the switch and directly connected to the reporter's computer during maintenance and had not been reconnected to the switch. Neither the reporter nor ESA personnel were aware of this. The information was transmitted when the reporter inadvertently pressed the return key while directly connected to the remote system. In the case of the early time stamp, we found that the clock on the reporter's personal computer was three minutes fast, and the web server posting the story used that time, giving the appearance of an early release. Because of these incidents, ESA has taken measures to improve security in order to preclude the actual or perceived early release of indicators.

Important among these measures is that ESA has transferred the responsibility for breaking off communications with external systems from the individual reporters to the ESA lockup director to minimize the chances of an early release. For each news service, ESA has installed a communications switch whose power source is controlled by a master power switch operated by the ESA lockup director. In addition, ESA now requires all reporters to ensure that the clocks on their personal computers are synchronized to Naval Observatory time to avoid having incorrect time stamps associated with news stories and thereby giving the perception of an early release of indicator data.

Information Technology Resources

The Retail and Wholesale Indicators Branch staff uses the information technology resources provided by the Economic Directorate's local area network (LAN) to produce the monthly Advance Retail Sales indicator. Staff from the Economic Statistical Methods and Programming Division (ESMPD) within the Economic Directorate is responsible for security and system administration of the LAN. The bureau has identified the LAN as a general support system in accordance with criteria provided by OMB Circular A-130, Appendix III. The LAN was accredited as a sensitive, but unclassified, system in August 2000. The general support security plan for the LAN identifies the Advance Retail Sales indicator as one of several production applications supported by the LAN.

During the monthly survey collection phase, branch staff access the survey data, which are keyed by bureau personnel and stored on a primary server and a backup server located at NPC. An additional backup server, which is accessible via the LAN, is also maintained at bureau

headquarters. Branch staff analysts access the NPC server from personal computers connected to the Economic Directorate's LAN. They perform edit and tabulation operations on the data, which is transferred over a secure connection between NPC and bureau headquarters.

Staff analysts also use the NPC server to generate ratios that serve as input to time-series and seasonal adjustment programs that are run from LAN personal computers on a Unix server at the bureau's Computer Center in Bowie, Maryland, to provide successively refined estimates of the indicator values. The Bowie facilities are accessed from bureau headquarters via a secure connection. Applications developed by the bureau are used to generate the final indicator values and commercially available application programs are used to prepare the associated publications, which are stored on a server at bureau headquarters.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this evaluation was to determine whether ESA and the Census Bureau have adequate internal controls to prevent the premature or unauthorized disclosure or use of Advance Retail Sales economic indicator data before it is released to the public via the ESA press release room. We selected the Advance Retail Sales indicator as the subject of this evaluation because of its importance to government, academic, and business organizations in their efforts to analyze economic policy, anticipate economic trends, predict demand for products, and forecast the direction of the economy.

Our field work was performed between July 2000 and April 2001. During this time, we reviewed written policies and procedures and identified the controls over the analysis, processing, and reporting of Advance Retail Sales data. We interviewed Census Bureau officials and staff and observed the procedures used to prepare the Advance Retail Sales estimates. In addition, we used the General Accounting Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM) as guidance to evaluate the effectiveness of controls associated with information technology resources used to prepare the Advance Retail Sales indicator. We also evaluated the management controls over personnel security for both the Census Bureau staff involved in preparing the indicator and ESA staff involved in releasing it.

We had originally planned to evaluate the general controls in place for the Economic Directorate's LAN. General controls are the structure, policies, and procedures that apply to an entity's overall computer operations and establish the environment in which application systems and controls operate. FISCAM identifies six major categories of general controls, with each category having an associated set of critical elements, and includes tables that provide guidance for assessing the effectiveness of the critical elements. Appendix A shows FISCAM's major categories of general controls, their purpose, and their critical elements.

As we were planning our evaluation, the bureau contracted for an information security risk assessment of its systems. The contractor decided to include the Economic Directorate's LAN and to use the National Security Agency's Information Security Assessment Methodology, which is similar to FISCAM. To avoid duplication of effort, we focused on application controls for the Advance Retail Sales application rather than on general controls for the LAN. The general control issues that the contractor raised have been resolved.

Application controls are the structure, policies, and procedures that apply to separate, individual applications systems, such as Advance Retail Sales and the other economic indicators, identified as applications in the General Support Security Plan for the LAN. An application system is typically a group of individual computer programs that relate to a common function, such as development of an economic indicator. Our evaluation of application controls is consistent with GAO's approach to application controls reviews, which emphasizes determining whether controls are in place to ensure that access privileges establish individual accountability and

proper segregation of duties, limit the processing privileges of individuals, and prevent and detect inappropriate or unauthorized activities. To accomplish this, we used the appropriate FISCAM tables relating to the access controls major category of general controls. In particular, for the Advance Retail Sales application, we evaluated logical access controls, physical access controls, and the use of system auditing to facilitate monitoring of file access, investigating apparent security violations, and taking appropriate remedial action. Furthermore, we evaluated the effectiveness of the software change control process as it relates to preventing and detecting inappropriate or unauthorized activities.

We held an exit conference with the Census Bureau on June 26, 2001. Prior to the exit conference, we discussed the information contained in this report with the Deputy Under Secretary for Economic Affairs and the bureau's Associate Director for Economic Programs. ESA and Census Bureau officials generally agreed with our findings and have already begun to implement some of our recommendations.

Our evaluation was conducted in accordance with the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency, and was performed under the authority of the Inspector General Act of 1978, as amended, and Departmental Organization Order 10-13, dated May 22, 1980, as amended.

FINDINGS AND RECOMMENDATIONS

I. Application Controls Should Be Strengthened

Logical access controls afford appropriate protection for development of the Advance Retail Sales indicator. These controls establish individual accountability, limit the processing privileges of individuals, and establish reasonable physical access controls for servers used in the development of the indicator. However, guidance on physical access to branch spaces during lockup needs to be clarified, software change control procedures need to be improved, and auditing software for detecting inappropriate access to resources on the server that contains final indicator information has not been used regularly.

A. *Physical access controls for servers on the LAN are reasonable, but guidance for personnel access to branch spaces needs improvement*

Physical access controls include locks, security guards, badges, alarms, and similar measures that help to safeguard computer facilities and resources from loss or impairment by limiting access to buildings and rooms where they are housed. The servers that are part of the Economic Directorate's LAN, as well as the servers in Bowie and NPC, which are accessed by analysts during development of the Advance Retail Sales indicator via the LAN, are housed in locked rooms to which access is physically restricted to only explicitly authorized personnel. In addition, access to branch office spaces during lockup is controlled in accordance with established procedures.

The Economic Directorate's *Procedures for Internal Control of Economic Indicator Data Prior to Press Release Time* requires printed material containing sensitive data to be stored in locked containers within branch spaces at the end of each workday and when not in use during the day. As an additional measure to prevent unauthorized access to sensitive economic data, staff from the Retail and Wholesale Indicators Branch ensure that printed reports are directed only to printers within the branch spaces.

The procedures contain a section titled, "Office Security Procedures," which specifies the process for ensuring that only authorized personnel have access to branch spaces where aggregate data are prepared. This document specifically states:

"All offices housing unpublished sensitive economic data will have controlled access for a fixed period of time to be established by the Branch Chief. During the period of time needed to prepare the release, no admission to the local branch areas where the aggregate data are prepared, will be permitted to unauthorized personnel. Formal notices, in English and Spanish, must be displayed at normal entry points to read:

NO ADMITTANCE/AUTORIZADO PERSONAL UNICAMENTE

During this time, the Branch Chief will designate only one entry point to the branch, which will be in compliance with fire regulations. A monitor is to be stationed close to the entry point to ensure enforcement of the “no admittance” policy. A sign-in/sign-out log will be maintained for non-branch personnel entering the area.”

During our evaluation, we observed two days of the Advance Retail Sales lockup process for the September 2000 release. When we arrived at the designated branch access point, appropriate signs were posted on the doors, and we were required to sign a log upon entry. In addition, we noted several occasions when non-branch personnel, who also regularly participate in the development of the indicator, signed the log as required upon entry to and exit from branch spaces. However, while observing the lockup process, we noted that a branch staff member exited the branch spaces through a doorway that was not designated as the access door and shortly afterward re-entered through the same door. This door was locked from the inside and required the use of a key to re-enter, and a “NO ADMITTANCE” sign was appropriately posted on the outside of the door.

The branch manager later confirmed that branch members, as well as authorized visitors, should use only the designated controlled access door to enter and exit the branch area during lockup. We believe that the procedures contained in the “Office Security Procedures” section of the internal control procedures should be modified to state explicitly that branch members are required to use only the controlled access door to enter and exit the branch area during lockup and that branch members should be reminded of this requirement. Explicitly stating and rigorously enforcing access requirements will increase the assurance that branch employees are not engaged in unauthorized disclosure of information. Strict enforcement will also ensure that normal entry points, which are locked at the start of a lockup period, remain locked. If a branch member were to exit through a locked door and that door would fail to close tightly, it could provide unauthorized persons an entry point to branch spaces and access to sensitive economic data.

Finally, we learned that occasionally personnel who are not authorized access to sensitive indicator data require access to branch spaces during lockup to repair copiers or perform other maintenance-related services. In these cases, the branch manager or supervisor ensures that a member of the branch accompanies such visitors and takes measures to prevent unauthorized access to sensitive data. However, the directorate’s internal controls document does not explicitly address protecting information when such visitors require access to branch spaces during lockup, and we believe that it should.

B. Logical access controls are appropriate

Logical access controls involve the use of computer hardware and security software to prevent or detect unauthorized access to resources by requiring users to provide unique user identifications, passwords, or other identifiers that afford predetermined privileges to access specific resources. These controls are used to restrict the access of legitimate users to specific systems, programs, and files needed to conduct their work, and to prevent unauthorized users from gaining access to computing resources. We found that ESMPD follows appropriate bureau-wide procedures pertaining to logical access controls as specified in the bureau's *Handbook for Information Technology Security* and the general support security plan for the LAN.

Access to LAN-based computing resources by branch analysts is controlled by unique user identification and password combinations, which are initially assigned and periodically changed in accordance with bureau-wide procedures. Users can access the LAN only if they have been assigned a valid user identification and password combination and can access only those servers for which they have been provided user identification and password combinations. Passwords are required to contain a specified minimum number of alphabetic and non-alphabetic characters. In addition, users are required to change their passwords upon initially logging on to a system and every 30 days thereafter. Password history files are maintained to ensure that passwords cannot be reused for at least 12 months.

Whenever any user makes a certain number of consecutive unsuccessful attempts to log on to a system, the LAN system administrators are notified, and subsequent log-on attempts from the user's account are disabled until an administrator reinstates the log-on capability. This mechanism allows an administrator to determine the cause of the access failure and to verify the user's identity before granting further access. For the Advance Retail Sales indicator, an extra level of access control is provided by the computer program used for editing and tabulating survey data, which is an additional user identification and password to enable access to the particularly sensitive survey data.

Supervisors within the Retail and Wholesale Indicators Branch follow bureau-wide procedures to obtain LAN and server access for newly hired staff, as well as to deactivate access privileges for staff who leave the branch. During our fieldwork, a branch employee resigned, and we verified that all of that employee's access privileges were promptly removed.

Finally, we determined that branch supervisors work with LAN administrators to ensure that analysts are provided access privileges only to the systems, programs, and data files needed to conduct their work. We reviewed directories on the servers used for development of the Advance Retail Sales indicator and found that access privileges are assigned only to members of the Retail and Wholesale Indicators Branch and to designated support staff from ESMPD. File access controls afforded by the various operating systems provide the mechanisms for assigning access privileges.

C. Application software change control is informal and lacks documented procedures

Application software has been designed to support development of the Advance Retail Sales economic indicator. This software consists of computer programs that have been developed by the bureau, as well as commercially available applications for which specific scripts have been written, to facilitate the generation of intermediate and final versions of the indicator.

Establishing and enforcing procedures for modifying application software and related scripts provides a level of assurance that only authorized programs and authorized changes are implemented. This can be accomplished by instituting policies, procedures, and techniques that help ensure that all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs are carefully controlled. Failure to implement effective change control measures presents a risk that security features built into the software could be inadvertently or deliberately circumvented or that unauthorized processing or malicious code could be introduced.

Although a process is in place for requesting changes to software used in the development of the Advance Retail Sales indicator (as well as other indicators) and ESMPD staff are aware of it, there are no written procedures for making the changes and performing and documenting appropriate tests on the modified software to ensure that only authorized changes are made. The application software for Advance Retail Sales has not required significant changes in the past several years, and an ESMPD programmer/analyst has been assigned to work with the Retail and Wholesale Indicators Branch to provide technical support and coordinate any necessary changes to the software. However, written procedures for application software change control are still needed.

A GAO report, *Information Security: Controls Over Software Changes at Federal Agencies* (GAO/AIMD-00-151R, May 4, 2000), underscores the general lack of effective software change control within federal agencies, including the Department of Commerce. Appropriate guidance for software change control within ESMPD needs to be developed, documented, and followed, particularly with respect to applications used in the development of economic indicators.

D. Auditing software has not been regularly used during lockup

Novell's Netware operating system provides a feature to create audit logs that contain a record of all accesses by users and applications to files containing pre-release information for Advance Retail Sales and several other indicators on the server where actual indicator data and reports are stored. ESMPD had enabled this feature on the publication server and developed an application program to filter the logged data and provide an indication of any potential unauthorized attempts to access the pre-release data. Although branch managers and supervisors have received instruction in the use of the application, they did not use it regularly to monitor resource access during and immediately following the monthly lockups because it was a relatively recent and evolving product with no documentation providing instructions to users. ESMPD network personnel had been using the application to scan the audit log files on the server during lockup to monitor access to the indicator data.

However, ESMPD has upgraded the operating system on this server to a new release of Netware, which will not provide audit logs in the format required by the audit application program. As a result, ESMPD officials have told us that they plan to evaluate several commercially available programs to replace the current audit application, install the selected program, and provide appropriate training for branch managers and supervisors who use the publication server. We support this effort and believe that ESMPD should provide written procedures to ensure that the selected audit program will be used properly by managers and supervisors during lockup.

E. Recommendations

We recommend that the Acting Director of the Census Bureau direct the Associate Director for Economic Programs to:

1. Ensure that the directorate's *Procedures for Internal Control of Economic Indicator Data Prior to Press Release Time* is modified to state explicitly that:
 - a. Branch members are required to use only the controlled access door to enter and exit the branch area during lockup, and branch chiefs are responsible for strictly enforcing this requirement.
 - b. A branch member is required to (1) accompany any visitors who are not authorized access to sensitive indicator data but who require access to branch spaces during lockup, and (2) preclude their access to the sensitive data.

The bureau has agreed with this recommendation and has agreed to provide us a copy of the updated document for review.

2. Ensure that branch members are aware of the requirements to use only the controlled access door during lockup and to accompany visitors not authorized to access sensitive indicator data.

The bureau has agreed with this recommendation. The Economic Directorate held a meeting with branch staff to re-emphasize these requirements and posted appropriate signs on the inside of every door in the lockup area.

3. Ensure that procedures for software change control are developed according to bureau and Department guidance and that they are followed, particularly with respect to applications used in the development of economic indicators.

The bureau has agreed with this recommendation. The Economic Directorate developed a document titled "Economic Directorate Current Surveys Change Control Model" and provided us a copy.

4. Ensure that a commercially available audit application is selected and installed as soon as possible and that written procedures are prepared and training on its use is provided.

The bureau has agreed with this recommendation and is exploring off-the-shelf software options. The bureau noted that until it finds an appropriate product, it will continue to use the existing software and monitor its output regularly.

II. Management Controls Over Personnel Security Need to Be Strengthened

Census Bureau employees who participate in the development of Principal Federal Economic Indicators, including the Advance Retail Sales indicator, as well as ESA employees who coordinate the release of these indicators, have advance knowledge of sensitive economic data that could affect or predict financial market activity. These employees could potentially profit from speculative market investments based on this advance knowledge. For Advance Retail Sales, employees know the final indicator values for up to a day and a half before its release to the public. The ESA employees who coordinate the release of all the Department's principal economic indicators via the lockup facility have access to final indicator data 15 minutes before the lockup begins. Consequently, the government needs to take measures to ensure that these employees are suitable for such positions of public trust.

In 1991, the Office of Personnel Management (OPM) issued Appendix A to 731 Subchapter 5 of the *Federal Personnel Manual* (FPM). This appendix provides guidance and criteria for classifying positions of public trust, such as those dealing with development of Principal Federal Economic Indicators, as high, moderate, or low risk. It also specifies the type of background investigation appropriate for each of the risk levels. However, the FPM was abolished in December 1993.

Since then, the bureau has developed its own guidance and criteria, which are consistent with Appendix A, and published them as chapter S-8 in the *Census Administrative Manual*. Chapter S-8 states that the immediate supervisor or manager having responsibility for a position has primary responsibility for designating the position's risk level. The current version of chapter S-8 was signed by the bureau director in December 1996. Tables 1 and 2 provide summary information from chapter S-8. Table 1 provides representative criteria for classifying positions as high, moderate, and low risk and indicates the corresponding type of investigation appropriate for each level of risk. Table 2 describes the types of investigation associated with the risk levels.

On December 28, 2000, OPM published in the *Federal Register* revised regulations concerning the classification of positions based on risk level and the associated background investigation requirements. These regulations, found at 5 Code of Federal Regulations Part 731, became effective on March 30, 2001; however, they do not provide details, such as those provided by FPM Appendix A, for classifying position risk levels and do not identify background investigation requirements for the various risk levels. Rather than including these details in the regulations, OPM has decided to offer federal agencies training on classifying position risk levels and determining appropriate background investigations. OPM's Federal Investigations Notice No. 01-08, dated March 19, 2001, provides details about the available training.

Additionally, because of the abolishment of the FPM, the regulation includes a section outlining OPM's and agencies' responsibilities for personnel security associated with the design, operation, and use of federal automated information systems, as required by OMB Circular A-130 (1996 version) and the Computer Security Act.

Table 1. Representative Risk Level Classification Criteria and Investigation Types in Chapter S-8 of the *Census Administrative Manual*

Risk Level	Representative Classification Criteria (Abbreviated from Chapter S-8)	Type of Investigation
High	<ul style="list-style-type: none"> (1) Positions involving duties of clearly major importance to the Census Bureau mission with major program responsibilities that affect the efficiency of the government. (2) Positions involving development or approval of plans, policies, or programs that affect the overall operations of the Census Bureau; that is, policymaking or policy-determining positions. (3) Positions involving fiduciary, public contact, or other duties demanding the highest degree of public trust. This includes positions in the Senior Executive Service; GS-15 positions that clearly involve fiduciary, public contact, or other duties demanding the highest degree of public trust; positions involving foreign duty; positions involving investigative compliance, inspection, or auditing responsibilities, regardless of grade, (4) Positions in which the incumbent is responsible for planning, directing, and implementing a computer security program, (5) Positions designated by the Director or a field office director. 	Background Investigation (BI)
Moderate	<ul style="list-style-type: none"> (1) Positions involving duties of considerable importance to the Census Bureau mission with significant program responsibilities that affect the efficiency of the government. (2) Positions involving duties that demand a high degree of confidence and trust. (3) Positions for which the incumbent is responsible for directing, planning, designing, operating, or maintaining a computer system, and whose work is technically reviewed by a higher authority at the Critical Sensitive or High Risk level to ensure the integrity of the system. 	Minimum Background Investigation (MBI)
Low	A position that does not fall into a higher sensitivity level.	National Agency Check with Inquiry (NACI)

Note: FPM Appendix A recommends that moderate risk positions undergo either an MBI or, preferably, a Limited Background Investigation, which is a more extensive investigation than the MBI.

Table 2. Description of Types of Investigations Associated With Risk Levels in Chapter S-8 of the <i>Census Administrative Manual</i>		
Risk Level	Type of Investigation	Description
High	Background Investigation	Consists of a subject interview, written inquiries, record searches, a credit check, and personal interviews with selected sources covering specific areas of a subject's background up to the past five years.
Moderate	Minimum Background Investigation	Consists of a subject interview, written inquiries, record searches, a credit check, and a law enforcement check covering the most recent five-year period.
	Limited Background Investigation	Consists of a subject interview, personal interviews with selected sources covering specific areas of a subject's background during the past three years, written inquiries, record searches, and a credit check.
Low	National Agency Check with Inquiry	Consists of record searches of national, state, and local law enforcement and investigative indices, as well as written inquiries and record searches covering specific areas of a subject's background during the past five years.

Although guidance has been available, the bureau has not ensured that appropriate background investigations for employees dealing with the Advance Retail Sales indicator have been completed and has not assigned appropriate levels of risk to positions held by these employees. Similarly, ESA has not verified that employees who coordinate the release of principal economic indicators have undergone appropriate background investigations.

Using guidance from the Department's Office of Human Resources Management, human resources personnel in Commerce bureaus are responsible for working with management to determine the risk level for each position. For low and moderate risk positions, human resources personnel are responsible for requesting the appropriate background investigation from OPM. For high risk positions, human resources personnel are responsible for providing background information to the Office of Security, which is then responsible for requesting the appropriate background investigation from OPM. In our efforts to identify the criteria that are used to determine appropriate risk levels and their associated background investigations, we noted a lack of guidance from the Office of Human Resources Management and the Office of Security, suggesting that the issue of appropriate risk levels and background investigations may exist elsewhere in Commerce. We have addressed this issue in our report, *Program for Designating Positions According to Their Risk and Sensitivity Needs to Be Updated and Strengthened*, Draft Inspection Report No. OSE-14486/August 2001, which includes recommendations for the Department to provide to operating units updated guidance for determining appropriate risk levels and their associated background investigations. The Department's Office of Security and

Office of Human Resources Management have agreed to provide updated guidance; thus, the bureau's Human Resources Division needs to ensure that their efforts to implement our recommendations are consistent with the Department's forthcoming guidance.

Finally, ESA has not provided employees having pre-release access to economic indicator data with guidance concerning legal and ethical restrictions on market investments based on advance knowledge.

A. Employees have not had appropriate background investigations

We reviewed the types of background investigations that were done for 27 bureau employees regularly involved in the development of the Advance Retail Sales indicator. Three were employees of the ESMPD, and 24 were employees of the Service Sector Statistics Division (SSSD). Twenty-two employees held positions classified as low risk, three held positions classified as moderate risk, and two held positions classified as high risk. Bureau guidance specifies that low risk positions should be subject to a National Agency Check with Inquiry (NACI), moderate risk positions to a Minimum Background Investigation (MBI), and high risk positions to a Background Investigation (BI). This is consistent with OPM guidance, which states that moderate risk positions could be subject to either an MBI or Limited Background Investigation.

For the 22 low risk positions, six employees had undergone the specified NACI; however, records provided by the Department's Office of Security could not identify the type of investigation done, if any, for the remaining 16. For the three moderate risk positions, two employees had received only an NACI and the other the required MBI. Both employees filling the high risk positions had undergone the required BI.

We also reviewed the types of background investigations done for another 169 employees of SSSD and found that 47 had no record of any investigation having been done. Furthermore, we found that for another 216 employees of ESMPD, 87 had no record of any investigation having been done.

In addition, we noted that two persons designated as alternate ESA lockup directors fill positions classified as equivalent to moderate risk, but have not undergone background investigations corresponding to the MBI.

As a result of our analysis, we conclude that management controls need to be strengthened to ensure that appropriate background investigations are completed for all employees within the Economic Directorate and for the ESA employees who coordinate the ESA lockup.

B. Risk levels for positions have not been properly assigned

We also found that risk levels assigned to positions held by some SSSD and ESMPD employees involved in developing the Advance Retail Sales indicator are inconsistent with the levels of responsibility and trust associated with their positions. For example, 23 employees regularly involved in the development of the indicator have access to the final data for up to a day and a half before it is released to the public through the ESA press room. Of these employees, only the Branch Chief's position is classified as moderate risk; the remaining positions are classified as low risk. This disparity in classification needs to be rectified, and these remaining positions should be reclassified as moderate risk because of the sensitive nature of the final indicator data and the requirement to prevent its disclosure prior to official release to the public. Moreover, the managers within the Economic Directorate should review and appropriately adjust the risk levels associated with all positions within the directorate.

In addition, the positions held by the ESA employees who coordinate the lockup have been classified according to the sensitivity criteria for national security positions. However, they do not handle national security information and should instead be classified according to the risk criteria for public trust positions.

C. Guidance concerning legal and ethical restrictions on market investments based on advance knowledge is not adequate

All Census Bureau employees are required to sign a sworn statement that they will abide by the data confidentiality requirements of Title 13 of the U.S. Code, which covers sensitive Census data. Employees within the Economic Directorate are regularly provided verbal and written reminders about the proper handling of data that is afforded protection from unauthorized disclosure and improper use by Title 13. Also, the bureau requires all new employees to attend a one-hour ethics briefing. Furthermore, Economic Directorate employees who are involved with economic indicators are provided a verbal semiannual reminder by their supervisor during performance reviews about the need to protect pre-release economic indicator data from public disclosure. However, these employees and other ESA employees who have access to pre-release indicator data are not provided written guidance that explains the ethical restrictions on investing in financial markets based on advance information that is not available to the public. The Standards of Ethical Conduct for Employees in the Executive Branch, 5 CFR Part 2635, contains section 703, Use of Nonpublic Information, which prohibits employee use of nonpublic data. This section also notes that, in addition to violations of this section, certain employee use of nonpublic information could also violate federal securities laws.

The Bureau of Labor Statistics (BLS), which also develops Principal Federal Economic Indicators, has issued Commissioner's Order No. 1-00 to provide guidance on how the Standards of Ethical Conduct for Employees in the Executive Branch apply to employees making financial

transactions with knowledge of BLS embargoed data. The order defines embargoed data as pre-release economic series data for the Principal Federal Economic Indicators produced by BLS, and specifically states that the standards prohibit employees who have access to embargoed data from using the data for private gain or allowing others to do so. It further states that employees may not take actions that could create an appearance that they are using nonpublic government information for private gain.

Additional guidance is given to help ensure that market investments made by such employees can in fact be made without violating or appearing to violate an ethical standard. For example, the order states that if an individual owns shares in a mutual fund, but does not participate in or receive advance knowledge of decisions regarding its portfolio, there would be no appearance of an ethics violation if transactions affecting the fund occurred while the individual has knowledge of embargoed data.

This order contains the type of specific guidance that should be provided to Economic Directorate employees who are involved in the development of economic indicators and to all ESA employees who have access to pre-release indicator data.

The Commissioner's Order is included as Appendix B.

D. Recommendations

We recommend that the Acting Director of the Census Bureau direct the Director of the bureau's Human Resources Division to:

1. Require division personnel responsible for position sensitivity classification to attend training classes described in OPM Federal Investigations Notice No. 01-08, March 19, 2001, to obtain an understanding of 5 CFR 731 risk classification and investigation requirements.

The bureau has agreed with this recommendation. The bureau's Human Resources Division will schedule appropriate training for its specialists.

2. Develop written guidance that reflects the position risk level classification and investigation requirements taught in the training classes mentioned above and distribute it to bureau managers so they can classify position sensitivity appropriately.

The bureau has agreed with this recommendation. Human Resources Division specialists will develop the written guidance in conjunction with security personnel after attending training classes.

We recommend that the Acting Director of the Census Bureau direct the Associate Director for Economic Programs to:

3. Reassess the position sensitivity codes for all employees to ensure that they reflect the appropriate risk designations based on the level of responsibility and trust associated with each position in accordance with guidance from the bureau's Human Resources Division.

The bureau has agreed with this recommendation. However, the bureau has indicated that positions held by all personnel working on indicator surveys will be designated as moderate risk, based on discussions with us. These discussions did not intend to convey that positions held by all personnel working on indicator surveys should be designated as moderate risk. Rather, we stated that those persons having access to the same information available to the branch chief should have positions designated at the same moderate risk level as the branch chief rather than low risk as currently designated. Some positions for personnel working on indicator surveys are currently designated as high risk, and other positions may also warrant a high risk designation. We reaffirm that risk designations should be based on the level of responsibility and trust associated with each position in accordance with guidance from the bureau's Human Resources Division.

4. Ensure that appropriate background investigations have been completed for all employees.

The bureau has agreed with this recommendation. However, the bureau's response notes that roles and responsibilities of human resources, security, and management with respect to risk designation and background investigations are not clearly defined and understood. Our report, Program for Designating Positions According to Their Risk and Sensitivity Needs to Be Updated and Strengthened, Draft Inspection Report No. OSE-14486/August 2001, recommends that the Department provide to operating units clear definitions of roles and responsibilities of human resources, security, and management with respect to risk designation and background investigations. Thus, roles and responsibilities for risk designation and background investigations should be made clear by forthcoming Department guidance.

We recommend that the Under Secretary for Economic Affairs:

5. Ensure that the position sensitivity codes for ESA employees who coordinate the release of economic indicators via the ESA lockup reflect appropriate risk designations rather than national security sensitivity levels currently assigned, and that background investigations appropriate for the risk levels are conducted.

ESA has agreed to work with the Office of Security and the bureau's Human Resources Division, which provides human resources support to ESA, to comply with this recommendation.

6. Request assistance from the Office of General Counsel's Ethics Division, and develop specific written guidance on how federal securities laws and the Standards of Ethical Conduct for Employees in the Executive Branch restrict employees' ability to engage in certain financial transactions with knowledge of pre-release economic indicator data.

The bureau has agreed with this recommendation and has issued written guidance for indicator staff on how the Standards of Ethical Conduct apply to employees making financial transactions with knowledge of Census Bureau Principal Economic Indicator data prior to public release.

Purpose and Critical Elements of Major Categories of FISCAM General Controls	
Entity-wide Security Planning and Program Management	
Purpose	<i>Provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls</i>
Critical Elements	<ul style="list-style-type: none"> Periodically assess risks Document an entity-wide security program Establish a security management structure and assign security responsibilities Implement effective security-related personnel policies Monitor the security program's effectiveness and make changes as needed
Access Controls	
Purpose	<i>Limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure</i>
Critical Elements	<ul style="list-style-type: none"> Classify information resources according to their criticality and sensitivity Maintain a current list of authorized users and their access authorized Establish physical and logical controls to prevent or detect unauthorized access Monitor access, investigate apparent security violations, and take appropriate remedial action
Application Software Development and Change Controls	
Purpose	<i>Prevent unauthorized programs or modifications to an existing program from being implemented</i>
Critical Elements	<ul style="list-style-type: none"> Ensure that processing features and program modifications are properly authorized Test and approve all new and revised software Control software libraries
System Software	
Purpose	<i>Limit and monitor access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system</i>
Critical Elements	<ul style="list-style-type: none"> Limit access to system software Monitor access to and use of system software Control system software changes
Segregation of Duties	
Purpose	<i>Establish policies, procedures, and an organizational structure so that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records</i>
Critical Elements	<ul style="list-style-type: none"> Segregate incompatible duties and establish related policies Establish controls to enforce segregation of duties Control personnel activities through formal operating procedures and supervision and review

**Purpose and Critical Elements of Major Categories of FISCAM General Controls
(Continued)**

Service Continuity

Purpose	<i>Ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected</i>
Critical Elements	Assess the criticality and sensitivity of computerized operations and identify supporting resources Take steps to prevent and minimize potential damage and interruption Develop and document a comprehensive contingency plan Periodically test the contingency plan and adjust it as appropriate

Commissioner's Order No. 1-00

**Commissioner's Order No. 1-00**

previous page

Date: January 27, 2000**Commissioner's Order No. 1-00****Subject:** Making Financial Transactions With Knowledge of Bureau of Labor Statistics (BLS) Embargoed Data

1. **Purpose.** To provide guidance on how the Standards of Ethical Conduct apply to employees making financial transactions with knowledge of BLS embargoed data, and on how BLS contract terms apply to contractors making financial transactions with such knowledge.
2. **Scope.** This Order applies to all BLS employees and contractors.
3. **Authority.**
 1. 18 USC 208, "Conflict of Interest Law", prohibits employees from taking official actions that will have a direct and predictable effect on their financial interests.
 2. The Standards of Ethical Conduct for Employees In the Executive Branch, 5 CFR Part 2635.703, states, "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."
 3. Part 2635.101(14) states, "Employees shall endeavor to avoid any actions creating the appearance that they are violating the law or the ethical standards set forth in this part."
 4. Commissioner's Order 3-93, "Confidential Nature of BLS Records", states, "Pre-release economic series data prepared for release to the public will not be disclosed or used in an unauthorized manner ... and will be accessible only to authorized persons."
4. **Reference Office.** Office of Administration, Division of Management Systems.
5. **Directives Affected.** Commissioner's Order 1-96, "Consumer Price Index Futures Contracts", is replaced by this Order.
6. **Definitions.** For purposes of this Order:
 1. **Embargoed data.** Embargoed data are pre-release economic series data for the Principal Federal Economic Indicators produced by the BLS.
 2. **Pre-release economic series data.** Pre-release economic series data are statistics and analyses that have not yet been cleared for release (that is, have not yet been officially released to the public), including but not limited to those that have a set date and time of release before which they must not be divulged.
 3. **Principal Federal Economic Indicator.** Currently, the following BLS data series have been designated by the Office of Management and Budget as Principal Federal Economic Indicators: the Consumer Price Index, Employment

Situation, Employment Cost Index, Producer Price Indexes, Productivity and Costs, Real Earnings, and U.S. Import and Export Price Indexes. This list of designations may be subject to change.

7. Background.

Financial markets often are influenced by the release of BLS Principal Federal Economic Indicator data. An employee or contractor with knowledge of embargoed data could benefit from financial transactions conducted during the time he or she has such knowledge.

8. Policy.

The Standards of Ethical Conduct for Employees of the Executive Branch prohibit employees who have access to embargoed data from using the data for private gain or allowing others to do so. Further, employees may not take actions that could create an appearance that they are using nonpublic Government information for private gain.

BLS contractors who have access to embargoed data are prohibited under the terms of their contracts from releasing the data to unauthorized individuals or gaining financially from knowledge of the data.

Accordingly, it would be a violation of law and ethics regulations for an employee, and it would be a violation of contract terms for a contractor, to:

1. use knowledge of embargoed data to buy or sell stocks, mutual funds, bonds, or futures, or to make other similar investments; or
2. disclose embargoed data to other persons, or advise or make recommendations to other persons based on knowledge of embargoed data.

9. Investments in Stocks and Bonds.

Employees have an obligation to avoid actions that create the appearance that they are violating an ethical standard, including the prohibitions against using non-public information for personal gain. If an employee purchased stocks or bonds at a time he or she had knowledge of embargoed data, it could create the appearance that the employee was using the data for personal gain. Therefore, employees should avoid purchasing and selling stocks and bonds during times that they have embargoed data. If an employee with knowledge of embargoed data purchases stocks and bonds on a regular basis (e.g., monthly), it would be advisable to arrange for these financial transactions to occur at times when the employee does not have knowledge of embargoed data. Taking these simple precautions should avoid the appearance of a violation of the ethics standards.

These precautions do not apply to purchases or sales of stocks or bonds when the individual does not control the timing of those transactions. For example, if an individual owns shares in a mutual fund but does not participate in or receive advance knowledge of decisions regarding its portfolio, there would be no appearance of an ethics violation if transactions affecting the fund occurred while the individual has knowledge of embargoed data. Similarly, if an individual has arranged for automatic reinvestment of stock dividends, or for automatic payroll allotments to savings bonds or the Thrift Savings Plan, there would be no appearance of an ethics violation if these automatic transactions occurred while the employee has knowledge of embargoed data.

10. Investments in CPI-Indexed Bonds.

In 1997 the U.S. Treasury and other institutions, such as The Tennessee Valley Authority and the Federal Home Loan Bank System, began to issue securities whose values are indexed to the Consumer Price Index (CPI).

18 USC 208 prohibits employees from taking official actions that will have a direct and predictable affect on their financial interests. Some official actions that affect a very large class of people, however, are not subject to this restriction. For example, it would not be a violation of 18 USC 208 for an Internal Revenue Service employee to determine answers to income tax questions even though the employee pays income tax, or for a Treasury Department employee to make decisions about interest rates even though the employee may have a variable rate mortgage that the decision might affect. Similarly, the CPI affects almost everyone in the country. Therefore, it is not a violation of 18 USC 208 for an employee to work in the CPI program even though the employee may own CPI-indexed bonds. Employees with knowledge of embargoed CPI information should recognize, however, that buying or selling CPI-indexed bonds while having embargoed CPI data may create an appearance of an ethics violation. If employees wish to buy CPI-indexed bonds, they should arrange to buy them at times when they do not have knowledge of embargoed CPI data.

11. Investments in CPI Futures.

In 1985 the Commodity Futures Trading Commission authorized the Coffee, Sugar, and Cocoa Exchange to trade futures contracts based on the CPI for Urban Wage Earners and Clerical Workers (CPI-W). The buying and selling of CPI futures contracts has been discontinued due to low inflation rates. Were inflation to rise, however, the Coffee, Sugar, and Cocoa Exchange might sell them once again.

If an employee who had knowledge of embargoed CPI data bought or sold CPI futures contracts and benefited financially, it could appear to be a violation of 5 CFR 2635.703, the regulation on use of non-public information for personal gain. Accordingly, BLS employees who have access to embargoed CPI data should not engage in the buying or selling of CPI futures contracts during the time they have access to the data. This precaution does not apply to transactions such as investments in a mutual fund that may buy or sell CPI futures contracts as only a percentage of its total investment portfolio.

12. Responsibilities.

Associate and Assistant Commissioners for the statistical program offices that produce Principal Federal Economic Indicators are responsible for assisting employees with questions on what information should be considered embargoed data for the purposes of this Order.

13. Disciplinary Actions.

Any willful unauthorized disclosure or use of embargoed data or other violation of the standards of ethical conduct by a BLS employee may constitute cause for the BLS to take disciplinary action against that employee including, but not limited to, reprimand, suspension, demotion, or removal. Any willful unauthorized disclosure or use of embargoed data by a BLS contractor may constitute cause for removal. Furthermore, unauthorized disclosure or use of embargoed data may be a violation of criminal law.

KATHARINE G. ABRAHAM
Commissioner of Labor Statistics



UNITED STATES DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. Census Bureau
 Washington, DC 20233-0001
 OFFICE OF THE DIRECTOR

SEP 7 2001

MEMORANDUM FOR Judith J. Gordon
 Assistant Inspector General
 for Systems Evaluation

Thru: Kathleen B. Cooper *KBC*
 Under Secretary for Economic Affairs

From: William G. Barron, Jr. *WGB*
 Acting Director

Subject: *Security Aspects of Advance Retail Sales Need Improvement,*
 Draft Inspection Report No. OSE-12754

Over the last several months, a number of meetings between U.S. Census Bureau personnel and members of the Office of Inspector General (OIG) have taken place concerning the preparation of the Advance Monthly Retail Sales indicator. It has been a very informative and beneficial process for both sides to examine the strengths and weaknesses of our current processes.

This memorandum transmits our comments on the draft report evaluating the security of the Census Bureau's Advance Retail Sales Principal Federal Economic Indicator. The first section describes some general comments, followed by specific responses to each of the report's recommendations.

General Comments

First, we believe the title you have selected for the report, "Security Aspects of Advance Retail Sales Need Improvement," suggests that there are some rather serious security shortcomings in the Retail and Wholesale Indicators Branch (where the survey is processed). I think your assessment of the security situation for retail sales is quite fair, and there are some shortcomings that need to be addressed. However, the report title implies significant security problems, rather than strengthening a system that is fundamentally sound. Unfortunately, many readers get little beyond the title page of government reports, and their interpretations of entire reports are shaped altogether too much by the title. We believe a more even-handed title would be "Steps to Strengthen Security Aspects of Advance Retail Sales Program Identified," or "Security of Advance Retail Sales Program—Additional Measures Recommended."

Second, although the early pages of the report touch on the issues that led to the focus on the indicator surveys, we feel they do not fully explain why the Census Bureau, and more specifically advance retail sales, was singled out to be the focus of the security inspection. The way the report is written may lead the reader to believe there was an existing problem with the

security of the advance retail sales indicator, such as a sensitive data leak from the Branch. Obviously, this is not the case, and we suggest further clarification to reflect that in the report. It is our understanding that the decision to inspect security at the Census Bureau was based on the view that if the OIG was going to inspect security procedures at the Economics and Statistics Administration (ESA), for completeness sake, it also should inspect security procedures surrounding the entire process of generating principal economic indicators, including activities performed at the Census Bureau. The Retail Branch was selected simply as an example of one of the branches generating principal economic indicators—not because of any suspicion about security within the Branch.

Finally, in the “Information Technology Resources” section, the last sentence on page 6 could imply to some readers that final indicator values are derived using commercially available software; this is not true. The generation of the final indicator values is not done using commercially available application programs, but a proprietary system developed and used exclusively by Census Bureau programmers. Once these values are available, we do use off-the-shelf packages to generate our publication.

Comments on the Recommendations

Application Controls Should be Strengthened

1. *Ensure that the directorate's Procedures for Internal Control of Economic Indicator Data Prior to Press Release Time is modified to state explicitly that:*
 - a. *Branch members are required to use only the controlled access door to enter and exit the branch area during lockup, and branch chiefs are responsible for strictly enforcing this requirement.*
 - b. *A branch member is required to (1) accompany any visitors who are not authorized access to sensitive indicator data but who require access to branch spaces during lockup, and (2) preclude their access to the sensitive data.*

We are updating the *Procedures for Internal Control of Economic Indicator Data Prior to Press Release Time* to reflect your suggestions. The updated procedure will be reissued to all divisions with indicator responsibilities in early September 2001. We will send you a copy of the updated procedures then. In regard to the access of personnel not authorized access to sensitive indicator data, it should be pointed out that these visits are infrequent and necessary to repair equipment critical to the development of the indicator for that month (for example, a computer or printer). Any repairs/maintenance on noncritical equipment is scheduled for after the lockup period. Nonetheless, the updated procedures document will address this situation.

2. *Ensure that branch members are aware of the requirements to use only the controlled access door during lockup and to accompany visitors not authorized to access sensitive indicator data.*

Despite the lack of formal documentation on these matters, we have always followed this procedure. Periodically, reminders were given to the staff for reinforcement. Since the first mention of your findings, we have taken steps to improve the enforcement of these rules. First, a meeting was held with the staff to re-emphasize the entire Directorate's *Procedures for Internal Control of Economic Indicator Data Prior to Press Release Time* document, highlighting the parts you recommend. In addition, during lockup, we now display a sign on the inside of every door, except the main door, that reads "DO NOT OPEN DURING LOCKUP. ENTER/EXIT ONLY THROUGH ROOM 2626 (main door)."

3. *Ensure that procedures for software change control are developed according to bureau and Department guidance and that they are followed, particularly with respect to applications used in the development of economic indicators.*

In response to previous discussions on this topic, the Economic Directorate has developed and documented a change control procedure for all current surveys, including the economic indicators. The Monthly Advance Retail Trade Survey (MARTS) has begun to use this procedure in production. See Attachment 1, *Economic Directorate Current Surveys Change Control Model*.

4. *Ensure that a commercially available audit application is selected and installed as soon as possible and that written procedures are prepared and training on its use is provided.*

Auditing software is an important feature for protecting the security of indicator data. Having the ability to review uses of our data files ensures that no outside users have access to the data prior to release. The system currently in place (the one described in the report) involves manual intervention and is only a short-term solution. The originally scheduled upgrade to the higher Novell NetWare operating system would have resulted in the loss of our ability to audit files. Consequently, the indicator areas have not been, and will not be, upgraded until a suitable alternative is implemented.

After discussions with experts at Novell, we are exploring third-party, off-the-shelf software options. Currently, the Economic Statistical Methods and Programming Division is reviewing and evaluating these options as one of their high-priority projects. Until they find a program that meets our needs, we will continue to use the old software and monitor output regularly.

Once auditing software is selected, we will prepare written procedures and train managers and supervisors on its use.

Management Controls Over Personnel Security Need to Be Strengthened

1. *Require division personnel responsible for position sensitivity classification to attend training classes described in OPM Federal Investigations Notice No. 01-08, March 19, 2001, to obtain an understanding of 5 CFR 731 risk classification and investigation requirements.*

The Human Resources Division (HRD) concurs with this recommendation. The HRD will explore available training for position sensitivity and schedule HRD Specialists for a position-sensitivity class. HRD Specialists will then develop training for managers as needed.

2. *Develop written guidance that reflects the position risk level classification and investigation requirements taught in the training classes mentioned above and distribute it to bureau managers so they can classify position sensitivity appropriately.*

Once HRD specialists have received in-depth training, they will develop written guidance in conjunction with the Security Office.

3. *Reassess the position sensitivity codes for all employees to ensure that they reflect the appropriate risk designations based on the level of responsibility and trust associated with each position in accordance with guidance from the bureau's Human Resources Division.*

Using the written guidance provided by the HRD, Census Bureau management will reassess the position sensitivity for all employees. In light of the findings by the OIG and subsequent meetings held with their representatives, it has been determined that all personnel working on indicator surveys will be classified with a moderate risk level.

4. *Ensure that appropriate background investigations have been completed for all employees.*

Census Bureau management, working with the HRD and the Security Office, will develop a plan for ensuring that appropriate background investigations have been completed for all employees. Our first priority will be to conduct background investigations on indicators staff, starting with the indicators staff working in the Service Sector Statistics Division (which includes MARTS). Working with the Security Office, we will develop a schedule for each of the indicators.

It should be noted that the HRD does not request background investigations for low, moderate, or high-risk positions. This is the sole responsibility of the Security Office. Management is responsible for assigning the appropriate risk level in conjunction with advisory guidance from the HRD.

5. *Ensure that the position sensitivity codes for ESA employees who coordinate the release of economic indicators via the ESA lockup reflect appropriate risk designations rather than national security sensitivity levels currently assigned, and that background investigations appropriate for the levels are conducted.*

The ESA fully agrees with this recommendation, recognizing the importance of maintaining a process that guarantees the integrity of public trust activities. The ESA will work with the Office of Security and the Office of Personnel to ensure that employees involved in the lockup have the appropriate position-sensitivity codes and background investigations.

6. *Request assistance from the Office of General Counsel's Ethics Division, and develop specific written guidance on how federal securities laws and the Standards of Ethical Conduct for Employees in the Executive Branch restrict employees' ability to engage in certain financial transactions with knowledge of pre-release economic indicator data.*

Dr. Frederick Knickerbocker, Associate Director for Economic Programs, drafted written guidance for indicator staff on how the Standards of Ethical Conduct apply to employees making financial transactions with knowledge of Census Bureau Principal Federal Economic Indicator data prior to public release. See Attachment 2, "Making Financial Transactions with Knowledge of Census Bureau Principal Federal Economic Indicator Data Prior to the Release of the Data." The document was signed by Acting Director Barron on August 22, 2001, and distributed to relevant Census Bureau staff.

Attachments

cc: US/EA