Office of Inspector General

U.S. Department of Labor
Office of Audit

Limited Scope Audit of Controls Over the Office of Workforce Security UI Weekly Claims Press

Final Report Number: 03-00-011-03-315
Date Issued: SEP 28 2000

TABLE OF CONTENTS

ACRONYMS

DDSS	Division of Data Systems Support
DLMS	Department of Labor Manual Series
DOL	U.S. Department of Labor
DRR	Division of Research and Reporting
ETA	Employment and Training Administration
FISCAM	Federal Information System Controls Audit Manual
GAO	General Accounting Office
LAN	local area network
NACI	National Agency Check and Inquiries
OFMA	Office of Financial Management Audits
OIG	Office of Inspector General
OIPA	Office Information and Public Affairs
OTIS	Office of Technology and Information Services
OWS	Office of Workforce Security
NIST	National Institute of Standards and Technology
SQL	structured query language
UI	Unemployment Insurance

EXECUTIVE SUMMARY

Background

The Unemployment Insurance (UI) Weekly Claims Press Release is issued by the U.S. Department of Labor (DOL) every Thursday morning at 8:30 a.m. The UI Weekly Claims Press Release contains the National total of initial claims for UI and is one of the leading economic indicators that may affect the financial and monetary markets. Thus, the data in the press release are sensitive and embargoed from the time it is first compiled on Tuesday afternoon until the official release time on Thursday morning. As a result, there is a need to protect the data and the UI Weekly Claims Press Release from unauthorized use and release while it is in embargoed status.

States report initial UI claims (the data) to the DOL, Employment and Training Administration (ETA). Within ETA, the Office of Workforce Security (OWS), Division of Research and Reporting (DRR) is responsible for collecting and compiling the data and producing the UI Weekly Claims Press Release. DRR completes its summarization of the data approximately 40 hours before the official release time. The day before the UI Weekly Claims Press Release is released, DRR produces a package which contains the UI Weekly Claims Press Release and supporting documents and distributes it to four high-level DOL officials for their review and information. Approximately 2 hours before the release, copies of the UI Weekly Claims Press Release are delivered by the print shop to the DOL Office of Information and Public Affairs (OIPA). OIPA is responsible for issuing the UI Weekly Claims Press Release at the prescribed time in the DOL press room.

Two computer systems are used in the UI Weekly Claims Press Release process. The data are collected and compiled on an OWS National Office computer operated by the Division of Data Systems Support (DDSS). The UI Weekly Claims Press Release and supporting documents are stored on an ETA local area network (LAN) server administered by the Office of Technology and Information Services (OTIS).

Audit Results

The Office of Inspector General (OIG) performed a limited scope audit to assess (1) the internal controls used to ensure the accuracy and completeness of the data used to produce the UI Weekly Claims Press Release, and (2) the internal controls over issuing the UI Weekly Claims Press Release and safeguarding the embargoed information against unauthorized use or early release to the public (prerelease). Our audit covered all aspects of the UI Weekly Claims Press Release process, from the compiling of the data by DRR to the release of the UI Weekly Claims Press Release by OIPA.

We found that controls were adequate to ensure the accuracy and completeness of the information contained in the UI Weekly Claims Press Release. The OWS staff responsible for preparing the UI Weekly Claims Press Release followed prescribed procedures and recognized the importance of protecting the embargoed information. However, we found several significant control weaknesses that must be corrected to adequately safeguard the information against unauthorized use or prerelease to the public.

There are internal control weaknesses in three principal areas: (1) Procedures used by OWS to process the data and produce UI Weekly Claims Press Release; (2) LAN server security; and (3) OIPA's press release procedures.

Data Processing and Report Production

- The embargoed data and UI Weekly Claims Press Release are processed and produced in an unsecured office environment.

- There are security vulnerabilities in the procedures used to deliver advance copies of the UI Weekly Claims Press Release package to the four high-level DOL officials the day before the UI Weekly Claims Press Release is officially released.

- A library management system is not used to track multiple versions of software production programs used to compile the data.

- There is no security clearance policy for individuals with access to embargoed data.

- Situations can occur where one person controls the entire UI Weekly Claims Press Release process.

- There are no formal procedures for responding to security incidents.

LAN Server Security

The ETA LAN server has several weaknesses that compromise the security level needed for embargoed documents.

- An excessive number of network administrators have access to the server containing the embargoed documents.

- The embargoed documents are not encrypted while stored on the server.

- Periodic security evaluations using a security software package are not performed.

OIPA Press Release Procedures

Hard copies of the UI Weekly Claims Press Release are not secure for a short period of time before the scheduled release to the press corps and there is no assurance that the press corps' computer modems are disconnected until the release time. A separate report, with recommendations for corrective actions, will be provided to OIPA.

Recommendations

Following are the recommendations for the Assistant Secretary for Employment and Training to correct the internal control weaknesses found in OWS:

- Create a restricted access office area for processing the embargoed data and producing the UI Weekly Claims Press Release. The restricted access office area should be isolated from the general office work area and should include a printer and safe.

- Strengthen the procedures used to deliver the advance copies of the UI Weekly Claims Press Release package by requiring:

  - a "Confidential Cover Sheet" (DL 1-350) be used for the packages containing embargoed data,

  - delivery be made only when the authorized DOL official is present, and

  - a signed receipt be obtained from the person receiving the package and the receipt be maintained on file by DRR.

- Implement a library management system to ensure that the latest versions of structured query language (SQL) programs are being used to produce the UI Weekly Claims Press Release, and store the SQL programs in a single directory with access limited to DRR staff responsible for processing the data.

- Develop and implement a security clearance policy for individuals with access to embargoed data. The policy should ensure that:

  - the sensitivity levels for all individuals, including contract staff, with access to embargoed data are classified as high risk,

  - the appropriate security clearances are obtained for these individuals, and

  - the sensitivity of position classifications and security clearances are continually monitored.

- Ensure that the DRR Reporting Team Leader and staff assistant responsibilities are always performed by different individuals.

- Develop and implement formal incident response procedures that ensure the proper officials are notified, appropriate action is taken to secure the data, and the incident is investigated to identify internal control weaknesses.

- Discontinue using the ETA LAN to store the embargoed UI Weekly Claims Press Release and supporting documents before the official release time. Instead, use a stand-alone computer located in a secure area, and ensure that:

  - procedures are developed and implemented to back up the files on a regular basis,

  - adequate access controls are used, and

  - all files containing embargoed information are encrypted.

Agency's Response

In the response to our draft report, the Assistant Secretary for Employment and Training stated that, while ETA did not view the findings as significant control weaknesses, they are important concerns and will be addressed as far as possible to implement the needed changes. ETA agreed that it would be desirable to create a restricted office area but at the current time there are severe limitations on space availability. The space where the embargoed data and the UI Weekly Claims Press Release are processed and produced is scheduled to be reconfigured in 2002. The current space plans will be reviewed to see if they can be altered at least to allow the unit to be located in an area that does not have major traffic. Additionally, ETA is looking into the technical feasibility of establishing a stand-alone system to store the embargoed UI Weekly Claims documents before release time. Concerning

security clearances, ETA stated that the Federal staff currently working on the UI Weekly Claims Press Release Process have been doing so for a long time. Therefore, ETA does not believe that a security clearance investigation is warranted for them. However, ETA will implement a policy to require a background investigation for any new employee who has access to the embargoed data. Concerning the process used to deliver UI Weekly Claims Press Release package, ETA stated that receiving DOL officials will be contacted before the package is delivered and this will negate the necessity for the "Confidential Cover Sheet" (DL 1-350) and a signed receipt from the recipient. ETA agreed to implement the remaining report recommendations. ETA's entire response is included at the end of this report.

Auditor's Conclusion

We disagree with ETA's conclusion that the findings in the report are not significant control weaknesses. Because the UI Weekly Claims Press Release contains embargoed data, it is critical that the data be protected until it is released at the prescribed time. ETA must recognize that in managing security of sensitive information, the risks associated with the UI Weekly Claims Press Release process should be identified and reduced. Unauthorized use and disclosure of the embargoed data and the UI Weekly Claims Press Release can effect the financial markets and damage DOL's reputation for managing sensitive information. Therefore, it is necessary that ETA take appropriate measures to protect the embargoed data and press release and minimize the risk against unauthorized use and disclosure. By failing to recognize the significance of the report findings and the need for timely corrective action, ETA is accepting more risk than is necessary under the circumstances. We believe that ETA must take immediate corrective action, as recommended in this report, to improve the security over the UI Weekly Claims Press Release process.

BACKGROUND, OBJECTIVES, AND SCOPE

Background

The UI Weekly Claims Press Release is issued by DOL to the press every Thursday morning at 8:30 a.m. The UI Weekly Claims Press Release contains the National total of initial claims for UI and is one of the leading economic indicators that may affect the financial and monetary markets. Thus, the data in the press release are sensitive and embargoed from the time it is first compiled on Tuesday afternoon until the official release time on Thursday morning. As a result, there is a need to protect the data and the UI Weekly Claims Press Release from unauthorized use or prerelease while it is in embargoed status. Users of the UI Weekly Claims Press Release include the Federal Reserve, the Council of Economic Advisors, Congress, business organizations, brokerage houses, investment bankers, and the media.

The source of the sensitive data in the UI Weekly Claims Press Release is the initial claims data reported by the states to ETA. An initial claim is a claim for UI filed by an unemployed individual after separation from an employer. Within ETA, the OWS DRR is responsible for collecting and compiling the initial claims data and producing the UI Weekly Claims Press Release. The states report the initial claims data on the ETA 538, "Advance Weekly Initial and Continued Claims Report." The majority of the ETA 538 data is reported via an electronic entry and transmittal system which is housed on state-operated OWS SUN computers. Each of the state computers is polled nightly by the OWS National Office computer to pick up the data submitted the previous day.

DRR completes its summarization of the initial claims data approximately 40 hours before the official release time. Once the data are summarized, DRR produces a package which consists of the UI Weekly Claims Press Release and supporting documents. The day before official release time, the UI Weekly Claims Press Release package is distributed to the Deputy Assistant Secretary for Employment and Training, the Director of OWS, the DOL Chief Economist, and the ETA Office of Public Affairs for their review and information. Copies of the UI Weekly Claims Press Release are delivered by the print shop to OIPA 2 hours before the release. OIPA is responsible for issuing the UI Weekly Claims Press Release every Thursday morning in the DOL press room.

Two computer systems are used in the UI Weekly Claims Press Release process. The initial claims data are collected and compiled on an OWS National Office computer operated by DDSS. The UI Weekly Claims Press Release and supporting documents are stored on an ETA LAN server administered by OTIS.

Objectives

The audit objectives were to assess

- the internal controls used to ensure the accuracy and completeness of the data used to produce the UI Weekly Claims Press Release, and
- the internal controls over issuing the UI Weekly Claims Press Release and safeguarding the embargoed information against unauthorized use or prerelease.

Scope

Our audit scope was limited to the processing of data that occurs at the OWS National Office to produce the UI Weekly Claims Press Release. The audit focused on the internal controls OWS has implemented over the process of producing and releasing the UI Weekly Claims Press Release. To accomplish our audit, we gained an understanding of the process and procedures used to produce the UI Weekly Claims Press Release. We interviewed key staff persons in OWS, DRR, DDSS, OTIS, and OPA and examined the UI Weekly Claims Procedures Manual. We also observed the actual data gathering and data entry procedures. Our audit did not include testing of computer controls. For the OWS Data System, we relied on the results of the computer testing procedures that were performed by OIG's Office of Financial Management Audits (OFMA) as part of the DOL's Fiscal Year 1999 Financial Statements audit. OFMA's computer controls testing followed the General Accounting Office (GAO) Federal Information System Controls Audit Manual (FISCAM) General Control procedures. For the ETA LAN, administered by OTIS, we interviewed staff to gain an understanding of automated controls over the server used to store the UI Weekly Claims Press Release and supporting documents.

The audit was performed in Washington, D.C. from March 2000 through April 2000 in accordance with generally accepted government auditing standards.

We used the following criteria in our audit:

- National Institute of Standards and Technology's (NIST), *An Introduction to Computer Security: The NIST Handbook*, and the NIST, *Guide for Developing Security Plans for Information Technology Systems.*
- GAO's FISCAM and Standards for Internal Control in the Federal Government.
- Department of Labor Manual Series (DLMS) 2, Chapter 300, Security Regulations.

FINDINGS AND RECOMMENDATIONS

1. The Embargoed Data and the UI Weekly Claims Press Release Are Processed and Produced in an Unsecured Office Environment

The embargoed data and the UI Weekly Claims Press Release are processed and produced in an unsecured open office environment. While we concluded that the personnel responsible for producing and reviewing the UI Weekly Claims Press Release are security-conscious, the level of security needed for such a sensitive press release is difficult to achieve in an open office environment. We found that computer screens were visible from aisles and adjoining cubicles. Charts and reports containing embargoed UI data were printed at a shared printer. We observed a maintenance person at the entrance of a cubicle while embargoed data was displayed on the computer screen. On two occasions we observed computer screens, displaying embargoed UI data, left unattended for brief periods of time. Also, copies of the embargoed UI Weekly Claims Press Release were placed in an unlocked cubicle cabinet. The cubicle was located near an open doorway that leads to a main corridor in the DOL building. Printouts containing embargoed data were stored in a safe located in an open work area.

Physical controls and safeguards are necessary to restrict access to embargoed and sensitive material. DLMS 2, Chapter 300, Section 352(a) states: "Employees using classified information or responsible for its custody will take every precaution to prevent deliberate or casual inspection by unauthorized persons." Section 353 prescribes security storage standards for confidential information which require the same storage practices as top-secret information.

The GAO FISCAM, Section AC-3.1 on access controls, considers that physical security controls over computer resources include computer terminals. Section AC-3.1 provides that unrestricted access be limited to personnel with a legitimate need to perform their duties. Access to sensitive areas by maintenance personnel should be restricted and controlled.

Because the UI Weekly Claims Press Release may affect the movement of financial markets, strict security measures are required to protect the embargoed data and press release prior to their official release. Processing the embargoed data and preparing the press release in an open office environment increase the risk of unauthorized access and prerelease.

Recommendation

We recommend that the Assistant Secretary for Employment and Training direct OWS to create a

restricted access office area for processing the embargoed UI data and producing the UI Weekly Claims Press Release. The restricted area should be isolated from the general office work area and should include a printer and safe.

Agency's Response

ETA agreed that it would be desirable to create a restricted office area but, at the current time, space availability is severely limited. The space where the embargoed data and the UI Weekly Claims Press Release are processed and produced is scheduled to be reconfigured in 2002. The current space plans will be reviewed to see if they can be altered to at least allow for the unit to be located in an area that does not have major traffic. ETA stated that area will be made as isolated "as possible in a cubicle setting" and the safe and a printer will be located in this area.

Auditor's Conclusion

We disagree with ETA's proposed corrective action plan and the time frame to achieve it. We believe that prompt action should be taken to ensure that the embargoed data and UI Weekly Claims Press Release is processed in a secured restricted office environment. This cannot possibly be achieved in a cubicle setting. ETA's response demonstrates that management is accepting an unnecessarily high level of risk over the next 2 years in its approach to safeguard the embargoed data and UI Weekly Claims Press Release. ETA should establish office space for this function that is physically restricted from the general work area and limits access to only authorized individuals.

2. There Are Security Vulnerabilities in the Procedures for Delivering the UI Weekly Claims Press Release Package to DOL Officials the Day Before the Official Release Time

There are security vulnerabilities in the procedures used to deliver the UI Weekly Claims Press Release package to designated DOL officials the day before the UI Weekly Claims Press Release is officially released. These vulnerabilities could compromise the security of the embargoed data and the UI Weekly Claims Press Release before the scheduled release time. We found that the required "Confidential Cover Sheet" (DL 1-350) is not used when the UI Weekly Claims Press Release package is delivered to the designated DOL officials. Additionally, the designated DOL officials are not required to be present when the UI Weekly Claims Press Release package is delivered to their offices, and signed receipts of delivery are not required from the persons receiving the package.

On Wednesday morning, approximately 24 hours before the official release time, the UI Weekly Claims Press Release package is hand-delivered to four designated DOL officials for their review and information. The UI Weekly Claims Press Release package contains copies of the embargoed UI Weekly Claims Press Release and supporting documents (graphs and a summary sheet). We identified two weaknesses in the procedures for delivering these packages.

- The required "Confidential Cover Sheet" (DL 1-350) is not used when delivering the Weekly Claims Press Release packages. Instead, "Confidential" is written on the package envelope. DLMS 2, Chapter 300, Section 371(c)(2) requires that the "Confidential Cover Sheet" be used when confidential information is carried within DOL. It is our position that using the "Confidential Cover Sheet" increases the awareness that the package is important and should be handled with the utmost security.

- The Weekly Claims Press Release package is normally hand-delivered to the designated DOL officials. However, procedures allow the package to be left on the DOL official's office chair if he or she is not present. A signed receipt of delivery is not required. DLMS 2, Chapter 300, Section 371(c)(4) provides that a receipt can be used to transmit confidential information if it is deemed necessary by the sender. We believe that using a signed receipt is necessary considering that the release package contains embargoed information. Additionally, security can be increased by implementing a policy that the release package only be delivered when the intended official is present.

Addressing these vulnerabilities will increase security over the delivery of the UI Weekly Claims Release package to DOL officials.

Recommendations

We recommend that the Assistant Secretary for Employment and Training direct OWS to strengthen UI Weekly Claims Press Release package delivery procedures by requiring:

- a "Confidential Cover Sheet" (DL 1-350) be used for packages containing embargoed data,
- delivery be made only when the authorized DOL official is present, and
- a signed receipt be obtained from the person receiving the package and the receipt be maintained on file by DRR.

Agency's Response

ETA stated that it will implement a procedure in which the authorized DOL officials will be notified in advance that the press release packages are available. The authorized DOL officials will then contact DRR staff and inform them when they are available to personally receive the package. Then the package will be hand delivered. This method will ensure that no one other than the recipients will have any possibility of gaining access to the press release package. ETA also stated that with this procedure, neither a security cover sheet nor a signed receipt will be necessary.

Auditor's Conclusion

ETA's response resolves part of the recommendation that delivery be made only when the authorized DOL official is present. To close the recommendation, ETA must provide documentation that the procedures were incorporated into the UI Weekly Claims Procedures Manual.

However, we disagree with ETA's response that the proposed procedure eliminates the need for the "Confidential Cover Sheet" DL 1-350, and a signed receipt. DLMS 2, Chapter 300, section 371(c), Confidential Information, specifically requires that "Hand-carried information will be covered from view by DL 1-350, Confidential Cover Sheet." Moreover, DLMS 2, Chapter 300, Section 371 requires a receipt be obtained for transferring top secret and secret material and it is optional for confidential material. Considering that the information in the press release package is sensitive and embargoed, a signed receipt from the authorized official should be obtained and kept on file for subsequent review and audit.

3. A Library Management System Is Not Used to Track Multiple Versions of Software Production Programs Used to Compile the Data

The DRR staff responsible for processing the embargoed UI data for the Weekly Claims Press Release has developed their own structured query language (SQL) programs which are used for production and analysis of the weekly claims figures. New SQL programs are developed or changed as needed. We found that there is no version control or production library to track and store the SQL programs. DRR staff stores different versions of the SQL programs in their individual directories. As a result, there is no assurance that the staff is using the most current versions.

According to GAO FISCAM, Section CC-3.1 on application software development and change control, library management software provides an automated means of inventorying software, ensuring that differing versions are not accidently misidentified. Library management software also provides a means of maintaining a record of software changes.

An up-to-date production library will provide assurance that DRR staff uses the latest SQL versions. It will also provide a means of maintaining a record of changes made to SQL programs so that unauthorized changes can be detected. Considering the small number of programs used by the DRR staff, this can be accomplished using either an automated or manual library management system.

Recommendations

We recommend that the Assistant Secretary for Employment and Training require OWS to:

- implement a library management system to ensure that the latest versions of SQL programs are being used to produce the UI Weekly Claims Press Release, and

- store the SQL programs in a single directory with access limited to DRR staff responsible for processing the UI data for the UI Weekly Claims Press Release.

Agency's Response

ETA responded that since the audit, one central directory was established on the computer and it will be used for processing all UI claims data. ETA stated that the older version of the program will only be kept until it is verified that the new version works. After verifying that the new version works, the older version will be deleted from the system to avoid confusion. Thus, it is not necessary to establish a formal library management system.

Auditor's Conclusion

ETA's response resolves the recommendations. The procedures described in the response basically establish a formal library management system. To close the recommendation, ETA should provide documentation that the procedures were incorporated into the UI Weekly Claims Procedures Manual.

4. There Is No Security Clearance Policy for Individuals with Access to Embargoed Data

There is no formal policy to ensure that all individuals with access to embargoed UI data and the UI Weekly Claims Press Release have the appropriate security clearances. We found that only 1 of 21 individuals who had access to the embargoed UI Weekly Press Release and/or related data had appropriate security clearances.

The Federal Personnel Manual FPM, Chapters 731 and 736, contains requirements for various levels of background investigations for employees with access to sensitive data. Every employee with access to sensitive data is required to undergo either a Special Background Investigation, Background Investigation, Limited Background Investigation, Minimum Background Investigation, or a National Agency Check and Inquiries (NACI) depending on the position risk level (sensitivity level).

Because data in UI Weekly Claims Press Release can affect the movement of the financial markets, we believe that all individuals who have access to the embargoed data should have a high-risk sensitivity level and Background Investigation security clearance in order to provide some assurance of employee integrity.

The following are details of our review of the security clearances performed on individuals who have access to embargoed data. We did not review the individuals' sensitivity level designations.

- There were six individuals in OWS, DRR with access to the embargoed UI Weekly Press Release and related data. Five of the individuals received the standard NACI security clearance when they were hired, and the sixth individual, the Division Chief, received a Background Investigation security clearance.

- There were six individuals in OWS, DDSS with access to the production server used to store the weekly claims data obtained from the states. This data forms the basis for the UI Weekly Claims Press Release and is considered embargoed. We were told that all six individuals received only the standard NACI security clearance.

- There were nine individuals in ETA's OTIS with access to the server used to store the Weekly Claims Press Release and supporting documents. Seven of these individuals were contract employees. We were told that none of the nine individuals had background checks.

Recommendations

We recommend that the Assistant Secretary for Employment and Training require that OWS develop and implement a security clearance policy for individuals with access to embargoed information in the UI Weekly Claims Press Release. The policy should ensure that:

- the sensitivity levels for all individuals, including contract staff, with access to embargoed data are classified as high risk,
- the appropriate security clearances are obtained for these individuals, and
- the sensitivity of position classifications and employee and contractor security clearances are continually monitored.

Agency's Response

ETA responded that most contractor staff in OWS, DDSS do not currently have security clearances, however, those with access to the embargoed data do sign affidavits. ETA also stated that contractor staff has high turnover rates and that the desired background investigation could cost $2,295 per employee, which increases the cost of the contract. However, ETA stated they will be recompeting the contract within a year and will add a requirement that the contractor provide this clearance for staff who has access to embargoed data.

For Federal staff, ETA responded that the individuals currently responsible for the UI Weekly Claims Press Release have been working on this project for a long time and therefore believe that a clearance investigation is not warranted for them. However, ETA stated that a policy will be implemented that requires a background investigation for any new employee who will have access to the embargoed data. ETA stated that contractors in OTIS would not require clearances if the Weekly Claims Press Release production is taken off the LAN. (See Finding Number 7.)

Auditor's Conclusion

We disagree with ETA's conclusion that background investigations are not warranted for existing Federal staff. There is no basis in sound security management practices for using the employee's length of service as a determining factor for obtaining security clearances. Decisions on security clearances should be based on access to embargoed data. This includes employees who produce the weekly claims report or who have access to the embargoed data. All personnel (employees and contractors) with access permission to computer resources in which embargoed data is stored also should have background investigations.

5. Situations Can Occur Where One Person Controls the Entire UI Weekly Claims Press Release Process

There are situations when the Reporting Team Leader in DRR controls the entire UI Weekly Claims Press Release process because of the small number of staff on the DRR Reporting Team. The process includes obtaining and entering weekly claims data from individual states, producing schedules with the National totals, and reviewing the end products.

Normally, the DRR Reporting Team staff assistant is responsible for obtaining and compiling the individual state figures and producing the initial schedules. The Team Leader is responsible for reviewing the embargoed data and advance copies of the UI Weekly Claims Press Release and distributing them to authorized officials.

We were told that there are situations when the staff assistant is on leave and the Team Leader takes over all the functions of the Weekly Claims Press Release process. We consider this situation an internal control weakness because there is no separation of duties.

The GAO Standards for Internal Control in the Federal Government, Control Activities Section, considers the division of responsibilities among staff an effective method to prevent a single individual from controlling all aspects of a critical process.

Recommendation

We recommend that the Assistant Secretary for Employment and Training require that OWS ensure that the Reporting Team Leader and staff assistant responsibilities are always performed by different individuals.

Agency's Response

ETA responded that there are always at least two people involved in the process of collecting, checking, and publishing data and there are four people on the DRR staff who are knowledgeable in the process. Thus, the DRR Division Chief and a person in another division are available to serve as back up to the Reporting Team Leader. It is a rare circumstance when one person collects the data and that same person plus the person who creates the publication check the data. Because it is a rare circumstance, ETA believes it can function well under the current staffing and backup for this task.

Auditor's Conclusion

ETA's response did not address our recommendation. To resolve the recommendation ETA must include in the UI Weekly Claims Procedure Manual a procedure that requires the Reporting Team Leader and staff assistant responsibilities always be performed by different individuals when key staff are not available.

6. There Are No Formal Procedures for Responding to Security Incidents

There are no formal procedures for responding to security incidents, such as unauthorized use or prerelease of embargoed data. DRR told us that there have been very few instances where the security of embargoed data has been jeopardized. In the event of an incident, common sense is used to handle the situation. Formal procedures should be developed and implemented to ensure that appropriate action is taken to secure the data and correct the cause of the incident.

Recommendation

We recommend that the Assistant Secretary for Employment and Training require OWS to develop and implement formal incident response procedures. The procedures must ensure that the proper officials are notified, appropriate action is taken to secure the data, and the incident is investigated to identify and correct internal control weaknesses.

Agency's Response

ETA's response stated that as a result of the audit, procedures have been developed and implemented for handling incidents. ETA provided a copy of the procedure that was included in the UI Weekly Claims Procedure Manual.

Auditor's Conclusion

This recommendation is closed.

7. The ETA LAN Server Administered by OTIS Does Not Have the Security Needed to Store the Embargoed UI Weekly Claims Press Release and Supporting Documents.

The UI Weekly Claims Press Release document, summary spreadsheets, and supporting charts are stored on a server that is part of the ETA LAN which is administered by OTIS. We identified several weaknesses that compromise the security level needed for embargoed documents. The following are details of the weaknesses found.

a. An excessive number of network administrators have access to the server containing the embargoed documents.

The GAO FISCAM, Section AC-2.1, provides that broad or special access privileges, such as those associated with operating system software that allow normal controls to be overridden, are only appropriate for a small number of users who perform system maintenance or handle emergency situations.

Because the ETA LAN serves all agencies within ETA, there are numerous network administrators with access to the server that contains the embargoed UI Weekly Claims Press Release. Although the embargoed UI Weekly Claims Press Release is stored in a directory with the proper access permission controls limited to the individuals responsible for the press release, network administrators also have access to the directory. Within OTIS there are two ETA employees and seven contract employees who have network administrator access to the server.

We believe that this is an excessive number of individuals with access permission to embargoed data and increases the risk of unauthorized entry into the system, prerelease, or manipulation of embargoed data in the UI Weekly Claims Press Release.

b. The embargoed documents are not encrypted while stored on the server.

The NIST, Special Publication 800-18, Section 6.GSS.2, defines logical access controls to include the use of encryption as a means to prevent unauthorized access to sensitive files.

Encrypting the embargoed UI Weekly Claims Press Release while it is stored on the ETA LAN server would increase assurances against unauthorized access or misuse.

c. Periodic security evaluations using a security software package are not performed.

The NIST, Special Publication 800-12, Section 9.4.1.1, states that automated tools can be used to help find a variety of threats and vulnerabilities, such as improper access controls or access control configurations, weak passwords, lack of integrity of the system software, or outdated software updates and patches.

System security requirements are constantly changing with new technologies. Therefore, network security should be periodically assessed using a security scanner or similar software that takes an automated, proactive approach to detecting security deficiencies present in the agency's computers and networks.

Therefore, we believe that OWS should not store the UI Weekly Claims Press Release and supporting documents on the ETA LAN because it does not have the internal controls needed to secure embargoed data.

Recommendations

We recommend that the Assistant Secretary for Employment and Training require OWS to discontinue using the ETA LAN to store the embargoed UI Weekly Claims Press Release and supporting documents. Instead, require OWS to use a stand-alone computer located in a secure area and ensure that

- procedures are developed and implemented to backup the files on a regular basis,
- adequate access controls are used, and
- all files containing embargoed information are encrypted.

Agency's Response

ETA responded that inquiries are being made with OTIS about the technical feasibility of establishing a stand-alone system and of still maintaining the needed backups and shared access within the staff versus what might be required to further isolate the areas of the LAN which are used to increase security. We expect to be able to accomplish this at the time of the office configuration in 2002.

Auditor's Conclusion

The recommendations can be resolved when ETA makes a management decision on the action they plan to take.