U.S. DEPARTMENT OF LABOR Employment and Training Administration Washington, D. C. 20210	CLASSIFICATION UI/Risk Analysis
	CORRESPONDENCE SYMBOL TEUM
	ISSUE DATE October 28, 1987
RESCISSIONS	EXPIRATION DATE September 30, 1988

DIRECTIVE : UNEMPLOYMENT INSURANCE PROGRAM LETTER NO. 42-87, Change 1

TO : **ALL STATE EMPLOYMENT SECURITY AGENCIES**

FROM : **DONALD J. KULICK**
Administrator
for Regional Management

SUBJECT : **State Employment Security Agency (SESA) Internal Security Risk Analysis Technical Assistance Guide**

1. **Purpose.** To transmit reissued Section of the Risk Analysis Technical Assistance Guide entitled "Final report - Vol 1: Findings, Analyses and Recommendations (Document E-1).

2. **References.** ET Handbook No. 376; UI Risk Analysis Guidance Documents distributed to SESAs in June 1982; UIPL NO. 34-87; and UIPL No. 42-87.

3. **Background.** Risk Analysis Technical Assistance Documents A-F were recently

transmitted to all SESAs along with UIPL No. 42-87. The attached Document E-1 entitled "Final Report - Vol 1: Findings, Analyses and Recommendations" was inadvertently omitted from that transmittal. The methodology contained in Risk Analysis Technical Assistance Documents A-F is intended to be used solely as a technical assistance guide at the SESA's discretion in the conduct of risk analyses. Such risk analyses may be completed as a separate review or as a part of an overall audit of agency operations, as established in OMB Circular No. A-128.

4. **Action Required.** SESA Administrators should ensure that the Risk Analysis technical Assistance Guide Document E-1 is distributed to appropriate staff.

5. **Inquiries.** Refer all questions to the appropriate Regional Office.

6. **Attachment.** Internal Security Risk Analysis Technical Assistance Guide Document E-1

(Attachment to UIPL 42-87, change 1)

DOCUMENT E- 1

RISK
ANALYSIS
TECHNICAL
ASSISTANCE
GUIDE

FINAL REPORT

COMPUTER SECURITY REVIEW AND RISK ANALYSIS

UNEMPLOYMENT INSURANCE BUREAU OPERATIONS

VOL 1: FINDINGS, ANALYSES AND RECOMMENDATIONS

presented to

STATE OFFICE OF EMPLOYMENT SECURITY
123 MAIN STREET
CAPITALTOWN STATE 12345

prepared by
EDP AUDIT CONTROLS, INC.

March 1983
Reissued
August 1987

DISCLAIMER

THIS COMPUTER SECURITY REVIEW AND RISK ANALYSIS HAS BEEN COMPOSED FOR EDUCATIONAL PURPOSES ONLY. AS AN INSTRUCTIONAL DOCUMENT. THIS ARTIFICIAL RISK ANALYSIS PRODUCT DOES NOT IN ANY WAY REFLECT THE PRACTICES OR PROCEDURES FOLLOWED BY ANY ACTUAL EXISTING STATE EMPLOYMENT AGENCY.

EXECUTIVE SUMMARY

This document is Volume 1 of a two-volume report which details the results of a risk analysis of the EDP-related aspects of the Unemployment Insurance Bureau claims processing operations at the State Office of Employment Security (SOES). This volume contains all findings, analyses and recommendations.

Chapter 1 of the report summarizes the major findings and recommendations.

Chapter 2 discusses in detail environmental and general risks faced equally by all elements of SOES.

Chapter 3 discusses risks due to specific problems with the policies, practices, procedures and organizational structure of the SOES Unemployment Insurance Bureau operation.

Volume 2 contains all risk analysis worksheets and descriptions of the methodologies employed.

During our security review and risk analysis of the Office of Employment Security's Unemployment Insurance Bureau Operations we observed the following major strengths:

1. SOES management is highly skilled in handling crises. This was clearly demonstrated during the 1982-1983 union strike. In our judgment, SOES's overall position after the difficulties was stronger than before.

2. SOES is moving towards the establishment of one of the most disaster-resistant claims processing setups that EDP/AC has ever observed. This will be achieved when each of the Unemployment

Insurance Bureau field offices carries out all aspects of claims processing.

We also observed the following major weaknesses:

1. There is a lack of effective separation between software support activities and Unemployment Insurance Bureau production operations.

2. The Threeville field office is deficient in physical access controls and is located in an area susceptible to floods and earthquakes.

3. Headquarters offices are located in an earthquake-prone area. An effective disaster recovery plan is needed.

4. Technical (hardware and software) security controls over the Comprehensive Unemployment Insurance System (CUIS) and Unemployment Insurance Bureau data files are inadequate.

TABLE OF CONTENTS

Section

CHAPTER 3 SPECIFIC ISSUES

CHAPTER 1

FINDINGS AND RECOMMENDATIONS

1.1. INTRODUCTION

This chapter contains a summary of all findings and recommendations resulting from the risk analysis. The finding number is the key to the to the section of the report in which the finding is discussed and the risk analysis calculations are explained. The finding number is equal to the section number followed by a dash followed by the ordinal number of the finding within the section. For example, Finding 3.9.2.4-3 would be the third finding in Chapter 3, section 3.9.2.4.

1.2 SUMMARY OF FINDINGS AND RECOMMENDATIONS

Finding 2.2-1: The Threeville Field Office is subject to flooding.
RECOMMENDATION: Prepare a formal contingency plan for the field office.

Finding 2.3-1: The risk of earthquake damage to the State Office of Employment Security Oneville facilities and their contents should be accounted for in a contingency plan.
RECOMMENDATION: Prepare a detailed contingency plan for SOES's Oneville facilities.

Finding 2.3-2: The Threeville field office building could collapse during an earthquake.
RECOMMENDATION: Prepare a contingency plan for the Threeville Field Office.

Finding 2.7-1: Headquarters offices are susceptible to unauthorized access.
RECOMMENDATION: Monitor the performance of the guard force and demand compliance with established procedures.

Finding 2.7-2: The wearing of badges at 456 Main Street is not enforced.
RECOMMENDATION: Enforce the wearing of badges at 456 Main street.

Finding 2.7-3: The State Supply warehouse is susceptible to unauthorized access.
RECOMMENDATION: N/A.

Finding 2.7-4: The Threeville Field Office is susceptible to unauthorized access.
RECOMMENDATION: Repair the gap in the rear exit door. Replace the photoelectric beam detectors with motion detectors.

Finding 2.7-5: The custodial services at the field offices perform their duties after hours and are not supervised by SOES personnel.
RECOMMENDATION: Have the custodial services perform their duties during normal business hours.

Finding 3.2.1.1-1: The Wage Record file is unprotected.
RECOMMENDATION: Provide secure storage for the Wage Record file at the Fourville field office.

Finding 3.2.1.1-2: The outside entrance to the Fourville field office is unmonitored during the early morning and late afternoon hours.
RECOMMENDATION: Ensure that the reception area is staffed at all times when the main entrance door is unlocked.

Alternatively, install a bell or other signaling device which will sound when the door is opened from the outside.

Finding 3.2.1.1.2-1: It is possible for a processor in the Adjustments and Overpayments Section to reactivated and pay a denied claim or to make an adjustment to a claim in a fraudulent manner.
RECOMMENDATION: Apply separation of duties between adjustment and overpayment processing and other aspects of claims processing.

Finding 3.2.1.2-1: The Wage Record file is unprotected.
RECOMMENDATION: Provide secure storage for the Wage Record file at the Twoville field office.

Finding 3.2.1.2-2: Outside doors to the Twoville field office (other than the main entrance) are unalarmend during business hours.
RECOMMENDATION: Install deadbolt locks on all but the main entrance door. issue keys to those who must use the doors in the conduct of their official duties.

Finding 3.2.1.2-3: Dry chemical fire extinguishers are provided for work areas in which CRT terminals are located.
RECOMMENDATION: Replace the dry chemical extinguishers with halon extinguishers.

Finding 3.2.1.2-4: Documents describing restricted access software are not give special protection in the Twoville field office.
RECOMMENDATION: Access to restricted software should be controlled through passwords or user security profiles, not through the secrecy of operating procedures. In the present situation, the restricted documents should be stored in locked desks or cabinets.

Finding 3.2.1.2.2-1: Correspondence processors can divert claim payments from their intended recipients in a variety of ways.
RECOMMENDATION: Determine patterns of claims processing transactions which would be carried out when fraud was being attempted. Flag for s special review all claims to which these patterns apply.

Finding 3.2.1.2.3-1: Passwords controlling access to CUIS Cash Disposition functions are not changed when employees who know them terminate their employment.
RECOMMENDATION: All access control keys (both logical and physical) should be returned to SOES or rendered unusable upon the termination of employees who possess them.

Finding 3.2.1.2.3-2: Passwords controlling access to CUIS Cash Disposition functions are sometimes written down by the clerks entrusted with them.
RECOMMENDATION: Establish and enforce a policy that passwords are not to be written down.

Finding 3.2.1.2.3-3: There is no effective control over mail which may be addressed to specific field office employees and which may contain checks made out to those employees.
RECOMMENDATION: Require that mail addressed to individual employees be opened by mailroom personnel or in the presence of a second party. Require also that employees not intentionally direct personal mail to the SOES address.

Finding 3.2.1.2.4-1: Address changes are accepted for Unemployment Insurance Bureau claimants over the telephone.
RECOMMENDATION: Use personal information to validate the caller's identity. Send notification of the address change to the old address.

Finding 3.2.1.2.5-1: Auditors in the Twoville field office report to the heads of the units they audit.
RECOMMENDATION: The auditors should report directly to the field office manager.

Finding 3.2.1.3-1: The main entrance of the Threeville field office is not monitored during the early morning and late afternoon.
RECOMMENDATION: Ensure that the reception area is staffed at all times when the main entrance door is unlocked. Alternatively, install a bell or other signaling device which will sound when the door is opened from the outside.

Finding 3.2.1.2.3-2: Documents describing restricted access software are not given special protection at the Threeville field office.
RECOMMENDATION: Access to restricted software should be controlled through passwords or user security profiles, not

through the secrecy of operating procedures. In the present situation, the restricted documents should be stored in locked desks or cabinets.

Finding 3.2.1.3.3-1: The Correspondence Unit auditor reports directly to the head of the Correspondence Unit at the Threeville field office. The data entry auditors report to the General Supervisor of the data entry units.
RECOMMENDATION: All auditors should report directly to the field office manager.

Finding 3.2.1.3.3-2: The Training/Auditing supervisor must relinquish most auditing responsibilities to the General Supervisor when training classes are in session.
RECOMMENDATION: Assign the audit responsibility to a single person reporting directly to the field office manager.

Finding 3.2.1.3.4-1: The backup A/C unit for the Threeville Data Center is not periodically tested.
RECOMMENDATION: Test the backup A/C unit on a regular basis.

Finding 3.2.1.2.4-2: Visitor access records are not kept at the Threeville Data Center.
RECOMMENDATION: Keep records of visitor access to the Threeville Data Center.

Finding 3.2.1.2.4-3: There are no underfloor water detectors at the Threeville Data Center.
RECOMMENDATION: Install underfloor water detectors at the Threeville Data Center.

Finding 3.2.3.1.2-1: It would be possible for a reviewer to form a conspiracy for purposes of fraud with an employer for whom he's responsible.
RECOMMENDATION: Provide more than on possible processor for each aspect of claims processing.

Finding 3.2.4-1: There is no effective control to ensure that employers who cease doing business or who leave the area are purged from the Master Employer File.
RECOMMENDATION: Investigate ways to improve the accuracy and currency of the master Employer File.

Finding 3.2.4-2: Although signatures are required on documents requesting Master Employer File updates, the

signatures are not verified.
RECOMMENDATION: Verify signatures on Master Employer File update requests.

Finding 3.3-1: There is no effective separation between CUIS development, testing and maintenance activities and production operations.
RECOMMENDATION: Provide for the effective separation of the development, maintenance and testing of application systems and the production operation of those systems.

Finding 3.3-2: It is possible for a single person to carry out all steps necessary to insert a software modification into the production CUIS system without independent review.
RECOMMENDATION: Ensure that all changes, additions and deletions to production CUIS software are reviewed by at least one analyst not involved in their preparation.

Finding 3.3-3: Journalization of CUIS transactions is incomplete.
RECOMMENDATION: Provide for complete journalization of CUIS transactions.

Finding 3.3-4: Restricted UIS subsystems are protected by secret clerk numbers coded into the software.
RECOMMENDATION: Use the ACF2 Security Software to protect restricted CUIS modules where possible.

Finding 3.3-5: The CUIS Software Support Group does not enforce periodic changes of passwords and permits the selection of passwords with mnemonic value.
RECOMMENDATION: Enforce periodic changes of passwords. Do not allow the use of Passwords with mnemonic value (other than perhaps pronounceability).

Finding 3.3-6: CUIS is not supported to the fullest extent possible by ACF2.
RECOMMENDATION: Use ACF2 to serve all the security needs of online CUIS subsystems.

Finding 3.4.1-1: CO2 is in use in the data center as a fire suppressant. It is potentially harmful to personnel.
RECOMMENDATION: Provide full flood halon protection for the entire data center.

Finding 3.4.1-2: There is no visitor sign-in policy at the data center.
RECOMMENDATION: Implement a visitor sign-in policy for the data center. Validate tape sign-out requests. Modify the badge token authorizing data center access.

Finding 3.4.1-3: The blue ID badge stripe which authorizes data center access can be easily forged.
RECOMMENDATION: In place of the blue stripe, use a difficult to duplicate marking such as an engraved design and attach it to the ID badge under the lamination. It then becomes impossible to add or remove this credential once a badge has been completely assembled, and the counterfeiting process is much more difficult than before.

Finding 3.4.1-4: Fire protection by CO2 is provided only for the underfloor areas of the data center.
RECOMMENDATION: Install a full-flood halon system in the data center.

Finding 3.4.1-5: The key to the storage area containing blank Unemployment Insurance Bureau benefit checks is kept on a hook near the computer console operator. The access list for the key contains 30 names.
RECOMMENDATION: Pare down the access list for the key to the Unemployment Insurance Bureau blank check storage area. Maintain all copies of the key in protected or continuously monitored storage locations.

Finding 3.4.1-6: There are no alarms and only hand-held fire extinguishers in the supply area adjacent to the main computer room.
RECOMMENDATION: Upgrade the fire detection and suppression equipment in the data center supply storage area.

Finding 3.4.1-7: There is no smoke exhaust capability in the data center.
RECOMMENDATION: Formalize the use of portable fans for exhausting smoke.

Finding 3.4.2-1: There is no provision for the real-time on-line reporting of incorrect password usage attempts to a security officer.
RECOMMENDATION: Provide for the online reporting of incorrect password entry attempts.

Finding 3.4.4-1: The data center has no policy requiring periodic changes to passwords. Users are allowed to specify their own passwords.
RECOMMENDATION: The data canter should require the use of randomly generated passwords which are changed at least once a year.

Finding 3.4.5.1-1: No authorization checks are made when tapes are signed out from the tape library.
RECOMMENDATION: Release tapes only to their owners or to persons authorized in writing by the owners.

Finding 3.4.5.1-2: Non-production tapes are scratched automatically when the retention date is reached.
RECOMMENDATION: Consult tape owners prior to scratching tapes whose retention dates have passed.

Finding 3.4.5.1-3: Tapes are not degaussed after scratching and prior to reuse.
RECOMMENDATION: Degauss all scratch tapes prior to reissue.

Finding 3.5.1-1: Secure areas used by the Accounting Department have walls which do not extend to the true ceiling.
RECOMMENDATION: Extend the walls of all secure storage areas to meet the true ceiling.

Finding 3.5.1-2: Benefit checks returned to SOES are not batched and present an easy target for abuse.
RECOMMENDATION: Batch returned checks in the mailroom prior to sending them to Cash Receiving. Then destroy the checks after generating the necessary accounting records>

Finding 3.8-1: When an audit is to be conducted, advance notice is given to the affected department.
RECOMMENDATION: As a matter of policy, give no notice of impending audit activity to the affected departments.

Finding 3.11.2-1: The storeroom used by the Mail and Distribution Department has walls which do not extend to the true ceiling as well as unalarmend exterior windows.
RECOMMENDATION: Extend the walls of all secure storage areas to meet the true ceiling.

1.3 SUMMARY OF ALES, SAFEGUARD COSTS AND SAVINGS

Finding Number	Subject Area of Finding	ALE Times 3.79 Equals 5-yr Loss Now ($)	Minus New 5-yr Loss	Equals Reduction in 5-yr Loss ($)	Compare to Costs	Savings ($) = Loss Reduction Minus Cost	Cost to Savings Ratio
32125-1	Auditor Conflct	57K	2.8K	54K	0	54K	0
32134-1	Backup AC Test	16K	0	16K	0	16K	0
32123-3	Personal Mail	3.4K	170	3.2K	0	3.2K	0
3451-1	Tape Lib ID Chk	2.3K	0	2.3K	0	2.3K	0
32312-1	Clms Revw Fraud	2.3K	110	2.2K	0	2.2K	0
38- 1	Audit Notice	1.1K	110	1K	0	1k	0
32134-2	Visitor Records	460	230	230	0	230	0
3211-2	4ville Entrance	2 .7M	0	2.7 M	300	2.7 M	1.1E-4
3212-2	2ville Entrance	1.9M	0	1.9M	300	1.9M	1.6E- 4
27-4	3ville Phys Sec	12M	0	12M	20K	12M	.002
3212-4	Protect Documts	284K	0	284K	2.2K	282K	.008
351- 2	Returned Checks	190K	0	190K	4.2K	186K	.023
3451-2	Tape Scratch	144K	36K	110K	11.4K	99K	.023
27-1	HQ Phys. Secur	380K	19K	360K	8.7K	350K	.025
341-2	Visitor Sign-in	1.8M	450K	1.4M	42K	1.4M	.030
351-1	False Walls	380K	190K	190K	6K	184K	.033
3.11.2-1	False Walls	38K	0	38K	2K	36K	.056
3212-3	Dry Chem Exting	10K	0	10K	1.2K	9K	.133
27- 5	Unsupv Janitors	190K	19K	170K	87K	83K	1.05
32124-1	Address Change	2.3K	110	2.2K	1.2K	1K	1.20
32112-1	Adj/Ovpmt Fraud	34K	3.4K	31K	22K	9K	2.44
3211-1	WR File Secur	2.3K	230	2.1K	1.5K	600	2.50
33-1	CUIS Dev/Prod	57K	5.7K	51K	38K	13K	2.92
22-1	3ville Flooding	307K	284K	23K			
23-2	3ville Quake	45K	30K	15K	29K	9K	3.22
23-1	Capitaltown quake	23K	6.1K	17K	16K	1K	16.0
324-1	Mster Empl File	11.4K	1.14K	10.26K	10.1K	160	63.1
341-7	Smoke Exhaust	0	0	0	3.7K	-3.7K	-1
341-1	C02 As Fire Sup	38	0	38	20K	-20K	-1

CHAPTER 2

GENERAL ISSUES

This chapter is concerned with findings related to general risks; that is, risks which affect the overall SOES Unemployment Insurance Bureau Computer Operation as opposed to a single department, branch, section, facility, asset, etc.

Each section in this chapter deals with a specific risk, such as fire, flood, etc. At the beginning of each section is a paragraph entitled *BACKGROUND AND INTRODUCTION*. This paragraph particularizes considerations involving the risk to the SOES environment and explains the techniques to be used in evaluating the impact of the risk in that environment.

Following the background and introduction is a series of one or more *FINDINGS* related to the subject risk. Each finding is a briefly stated conclusion about the effect of the risk on SOES Unemployment Insurance Bureau Computer Operations.

After the finding is a paragraph entitled *RELATED CONTROL STANDARD*. This is a statement of a generally accepted principle of good security practice. Several professional EDP auditing groups have prepared codified lists of standards which have been published in the literature and subjected to peer review. One of the earliest of these is the "Computer Control Guideline" first published by the Canadian Institute of Chartered Accountants in 1970. Another is "Control Objectives - 1980" published by the EDP Auditors Foundation for Education and Research (EDPAFER). It is this latter document from which the control standard references used in this report are taken.

The primary purpose for stating the EDPAFER minimum requirement related to each finding is to demonstrate that in fact the finding does represent a situation in which a requirement is not being met.

A second reason for stating the EDPAFER requirement for each finding is that comments are often made that certain findings are not related to computer security issues.

Our view, however, is that computer security embraces *all* issues which must be addressed to assure the *continuous*

and *reliable* operation of a computer center and the timely accomplishment of all its processing.

Clearly this is a very broad objective. It encompasses such concerns as ensuring that necessary supplies are delivered on time; employing a detailed software development methodology to ensure that production applications are virtually bug-free from the beginning; and providing for good employee morale.

Computer security also embraces the more obviously security-related issues such as visitor access controls, data file protection, sign-on passwords and so forth.

When taken out of the context of an integrated ADP security program, individual findings and issues may seem to be nothing more than matters of ordinary good practice and totally unrelated to security and integrity. Those who feel that such issues are irrelevant to security should stop to consider the overall impact of each finding.

If the computer center runs out of printer paper because of a poor inventory control system, job output cannot be printed and SYSOUT must be dumped to tape before it fills up its allotted space. Management does not get the information from this output on schedule and important business decisions are delayed, perhaps beyond firm deadlines. Proper management of supplies may not seem like a matter of security but it clearly can be as this example shows.

Lack of a detailed software development methodology can lead to applications which are poorly designed, cryptically coded and sparsely documented. Such applications must be frequently removed from production due to bugs. The software maintenance personnel spend may unnecessary hours attempting to thread through the cryptic code and read between the lines of the sparse documentation. The production output that does get into the hands of the user may contain errors and lead to bad decisions.

Failure to ensure good employee morale can lead to purposefully careless work habits, strikes (if the employees are unionized), fraudulent destructive activity and/or a high employee turnover rate. Bad employee morale, if not avoided, can thus lead to anything from a loss of efficiency to the total paralysis of the computing operation.

The next paragraph associated with each finding is entitled *DISCUSSION*. This paragraph expands upon and provides the

details necessary to understand the finding.

Following the discussion is a *RISK ANALYSIS* paragraph which describes the calculations which were carried out to compute the annual loss expectancy. These calculations involve **estimates** of the annual frequencies with which undesirable events occur and **estimates** of the extent of monetary loss which will result from the occurrence of the events. The calculations are inexact and the results are rounded to two significant figures to reflect this fact.

Next is a paragraph called *SUGGESTED SAFEGUARDS AND COST BENEFIT ANALYSIS*. In this paragraph additional safeguards are proposed to reduce the expected loss and/or the annual frequency estimate associated with the finding. The cost of installing and operating each additional safeguard is compared to the reduction in the ALE it will bring about. Again, the results of calculations are rounded to reflect their inexactness.

Finally, there is a *RECOMMENDATION* paragraph. Recommendations are specific and based on the cost-benefit analysis of the preceding paragraph.

2.1 FIRE

HEADQUARTERS

The headquarters buildings do not have an automatic fire sprinkler system. Each floor has portable fire extinguishers with an ABC fire rating. A comprehensive fire safety program is being followed. The facilities are inspected by the fire department once a month. All the employees are made aware of the evacuation producers and specially assigned personnel are trained to assist in the evacuation of the building. The local fire station is within a one mile radius and the response time is less than one minutes.

999 BACK STREET

The State Supply Warehouse building is equipped with automatic fire sprinkler systems throughout the work area. When the sprinkler system is activated, an alarm is generated and sent directly to the XYZ Security Services central control office. They contact the local fire station. The fire department inspects the warehouse once a year. Each floor has portable fire extinguishers with an ABC rating. A comprehensive fire safety

program is being followed. All employees are made aware of the evacuation procedures and specially assigned personnel are trained to assist in the evacuation of the building. The fire department is within a one mile radius and the response time is 45 seconds to one minute.

FOURVILLE

The Fourville Field office does not have an automatic sprinkler system in the work area. The main floor has portable fire extinguishers with ABC fire ratings. A comprehensive fire safety program is being followed. The field office is periodically inspected by the local fire department. All the employees are made fully aware of the evacuation procedures. In the event of an emergency, the department supervisor leads his own unit out safely. The local fire station is within a two mile radius and the response time is less than five minutes.

Twoville

The Twoville field office has automatic fire sprinkler systems throughout the work area. The field office is equipped both with ABC and Halon fire extinguishers. A comprehensive fire safety program is being followed. The facilities are periodically inspected by the fire department on request by the field office manager. All the employees are made aware of the evacuation procedures. The local fire department is within a on mile radius and the response time is one minute or less.

THREEVILLE

The Threeville field office has automatic fire sprinkler systems throughout the area. The field office is equipped with ABC rated fire extinguishers. A comprehensive fire safety program is being followed. The facilities are inspected once every three months by the local fire department. All the employees are made aware of the evacuation procedures and specially assigned safety monitors are trained to assist in the evacuation of the building. The fire department is less than one mile away from the field office and the response time is less than one minute.

2.2. FLOODS AND OTHER WATER DAMAGE

HEADQUARTERS

Since the headquarters of the Office of Employment Security are located above sea level, the likelihood of a flood occurring is

minimal. The mean sea level in one hundred years will reach an estimated height of 5 ft. 6 in. at high tide according to the National Oceanic and Atmospheric Administration. Therefore the threat of any damage to the building structure or the contents would be significant.

999 BACK STREET

Since the State Supply warehouse is located above sea level, the likelihood of a flood occurring is minimal. The mean sea level around the nearby body of water will reach an estimated height of 5ft. 6 in. at high tide every 100 years according to the national Oceanic and Atmospheric Administration. Therefore the threat of any damage to the building structure or the contents would be insignificant

FOURVILLE

The State Department of Water Conservation is conducting a flood control project in Fourville. The Big Fourville Creek and the Little Fourville Creek flow through the town. The Little Fourville Creek flood flow is diverted from Fourville to Fiveville Count. The Big Fourville Creek flows to the north and then west, where it joins the Big River. Fiveville County maintains the levees and the passage gates while the State Department of Water Conservation is responsible for the inspection, operation and maintenance. The inspection of the levees occurs twice a year, and they are considered to be strong and well maintained.

TWOVILLE

The Hat Rive and the Wood River are not a direct threat to the two of Twoville. If a flood occurred, Woodtown, which lies directly across the Wood River from Twoville, would be flooded by the Hat River and the Wood River would continue to flow South. The Wood River Dam and the Old Davis Dam are both considered to be good levees. They are inspected twice a year and are well maintained.

THREEVILLE

The Threeville Field office is located in a flood zone designated as (AO) on a map produced by the U.S. Department of Housing and Urban Development, Federal Insurance Administration. The probability of a flood occurring in this zone is one in a hundred years (.01). Zone AO refers to an area which should experience a 1-3 foot flood level not more than once every hundred years. The

potential source of flooding is the Dynamite Creek.

FINDING 2.2-1:

The Threeville Field Office is subject to flooding.

DISCUSSION:

When a flood occurs, the depth of the floodwaters would reach a maximum level of three feet. Since the field office is located at ground level, the floodwaters would reach the main floor level, and damage the contents of the building.

RISK ANALYSIS:

The Annual Frequency Estimate (AFE) of a flood reaching its maximum depth of 3 feet is .01.

The probability of floodwaters reaching the Threeville Field Office main floor level is relatively high, because the field office is at ground level.

A reasonable estimate of cleanup would be $10K. This cleanup cost includes the drying and shampooing of the carpets in the Threeville Field office. The replacement cost for furniture, book shelves, desks and supplies, would be about $500 per employee. Also, each desk houses a CRT terminal. The standard desk measures 30in. (or 2ft 6in). Since the floodwaters reach maximum depth of three feet, the CRTs would be damaged; the estimated loss is the number of CRTs to be replaced multiplied by the remaining lease obligation per CRT.

The field office's vital records would be safe from water damage, because they are or could easily be stored above the three foot level.

In the absence of a contingency plan, SOES would lose about two weeks of operations while the cleanup was underway.

The total loss is the total cost of recovering form the flood. This is equal to the clean up cost plus the cost of replacing office furniture and equipment plus the reaming obligation on the ADP equipment lease plus the cost of the 1-1/2 weeks of overtime which could be eliminated by a good disaster recovery plan (part of the contingency plan).

The cost of office furniture and equipment is 128 staff x $500 =

$64K.

The cleanup cost should not exceed $10K.

The remaining 3 year lease obligation based on a monthly charge of $17,866 is $643K.

The cost of 1-1/2 weeks of overtime for a staff of 128 at an average $6.50 per hour salary and 25% overhead is 1.5 wks x 40 hrs/wk x $6.50/hr x 128 staff x 1.5 overtime x 1.25 overhead = $94 K.

The total loss is then $64K + $10K + $643K + $94K = $810K.

The ALE is .01 % x $810 = $81K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The safeguard is a contingency plan which would expedite recovery activities and save about 1.5 of the 2 weeks which would otherwise be required to clean up.

The yearly savings (not counting the cost of contingency plan development) will be the AFE multiplied by 2/3 of the overtime costs (all but 1/2 week)or .01 x 2/3 x $94K = $6.3K.

The ALE reduction will be $81K - $6.3K = $75K.

The cost of contingency planning is determined after all ALE reductions generated by the existence of the plan have been calculated. This is done on the multiple effects worksheet in Appendix C.

See the risk analysis worksheets in Section B.1 of Appendix B.

RECOMMENDATION

Prepare a formal contingency plan for the field office.

2.3 EARTHQUAKES

HEADQUARTERS AND 999 BACK STREET

The headquarters buildings are located in a grade C intensity area. Grace C is referred to as a very strong intensified area that can expect substantial damage from an earthquake. This

information corresponds to intensity readings greater than 6.0 on the Richter scale. These buildings have three stories. There is an underground parking garage below 123 Main Street.

The State Supply Warehouse building is located in a grade D intensity area. Grade D is also referred to as a strong intensified area that can expect some damage from an earthquake.

FINDING 2.3-1:

The risk of earthquake damage to the Office of Employment Security Capitaltown facilities and their contents should be accounted for in a contingency plan.

RELATED CONTROL STANDARD 5137(Q)(4):

In the event of a disaster or disruption, the computer facility and the backup facility must have the capability to function normally with minimal delay or lost processing time.

DISCUSSION:

In the Capitaltown area, the probability of an earthquake occurring is high. A contingency plan should be drafter to ensure continuity of operations for the Office of Employment Security headquarters offices.

RISK ANALYSIS

The annual frequency estimates for an earthquake larger than 6.0 on the Richter Scale is .02. This translates into a probability of occurrence of two in one hundred years. The AFE would be lower except for the fact that there has been no serious earthquake activity in the area in recent times and current research indicates that the longer the period of inactivity along a fault line, the higher the probability of a strong earthquake.

An earthquake of magnitude 6.0 or greater would cause major disruption to Office of Employment Security operations. Without a contingency plan, it is estimated that operations would be halted for approximately four weeks. Time would be needed for getting additional office space, moving in, and starting up operations.

Once operations were resumed, the Office of Employment Security would have to pay overtime to many production employees to make up for lost time. Because the Threeville data center can continue to accumulate Unemployment Insurance Bureau transactions while the

central computer in Capitaltown is disabled, DDE operations would not be affected. The overtime would apply to approximately 170 non-DDE processors at HQ and in the field offices.

The cost of overtime would be 4 wks x 40 hrs/wk x $6/hr x 170 staff x 1.5 overtime x 1.25 overhead = $310K.

The ALE is then .02 x $310K = $6.2K.

SUGGESTED SAFEGUARD AND COST-BENEFIT ANALYSIS:

The suggested safeguard is to draft and implement a contingency plan which will allow SOES to move to emergency office space and restart operations within one week of a major disaster.

This will reduce the ALE by 75% to $1.6K.

The cost of developing a contingency plan will be determined on the basis of the total ALE reduction it will generate. For 5 years, this reduction is $6.2K x 3.79 - $1.6K x 3.79 = $17K. This and an annual testing and updating expense of $1.5K. The total 5-year cost would be 3.79 x $1.5K + $10K = $16K.

The 5-year savings is then $17K - $16K = $1K.

See the risk analysis worksheets in Section B.2 of Appendix B.

RECOMMENDATION:

Prepare a detailed contingency plan for SOES's Capitaltown facilities.

FOURVILLE AND TWOVILLE

The Fourville field office is located in a single story structure which is also occupied by a restaurant and a real estate agency.

The Twoville field office occupies one third of the space in a converted warehouse. It is a brick-faced, wood frame building with dropped ceilings. One third of the building is vacant and the other one third is occupied by a reputable restaurant.

Both the Fourville and Twoville field offices are located in areas designated as zone 3. Zone definitions are taken from the Deterministic Seismic Hazard Map of the U.S. after Algermissen. In this vicinity, there is no history of earthquakes of a high

enough magnitude to inflict significant damage. Between 1900 and 1974 there were no earthquakes of intensity greater than 5.7 on the Richter Scale.

The Fourville and Twoville field offices are located in a relatively safe valley area in which the soil is made up of sand and gravel. In conclusion, if an earthquake were to occur in this area, it would result in little or no damage to SOES facilities, and therefore is of minimal concern.

THREEVILLE

The soil in the Threeville area is made up of loosely filled coarse grain earth. If an earthquake greater than 6.0 on the Richter Scale were to occur for more than one minute (continuous shaking), the ground water would liquefy the pore spaces and destroy the soil structure. This would cause the soil to essentially become quicksand and parts of the building could collapse. The Tectonic fault is approximately one mile east of Threeville. The fault extends from Narrow Creek southward into Lakeside County. Most of the known activity of the Tectonic fault is further south away from the city of Threeville.

FINDING 2.3-2:

The Threeville field office building could collapse during an earthquake.

DISCUSSION:

Because the terrain around the city of Threeville is made up of loosely filled coarse grain earth, the SOES field office building could collapse during an earthquake.

RISK ANALYSIS:

The AFE for an earthquake of magnitude 6.0 or greater at Threeville has been set at .01. In the absence of a contingency plan, such an earthquake would halt Threeville field office operations for the 4 weeks it would take to locate emergency space, move in and reconfigure all ADP and communications equipment.

Claims processing activities at HQ, Fourville and Twoville would also be affected because these activities require that the Threeville Data Center be in operation. The ALE will be the dollar equivalent of 4 weeks' overtime for about 300 claims

processing personnel plus the cost of office furniture and supplies for the Threeville staff ($64 from Finding 2.2-1) plus the cost of the remaining 3 years lease obligation for ADP equipment at Threeville ($643K from Finding 2.2-1).

The overtime cost is 4 wks x 40 hrs/wk x $6/hr x 1.5 overtime x 1.25 overhead x 300 staff = $540K.

The total ALE is then .01 x ($540K + $64K + $643) - $12K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The suggested safeguard is a contingency plan which will allow the Threeville field office to reestablish itself in new space within one week of a disaster.

The savings (not including the cost of contingency plan development) will be 75% of that portion of the ALE which is due to overtime costs or .75 x .01 x $540K = $4.1K.

The ALE reduction is then $12K - $4.1K = $7.9K.

The cost of the contingency plan development is determined after all ALE reductions brought about by that safeguard have been calculated. This is done on the multiple effects worksheets of Appendix C.

See the risk analysis worksheets in Section B.3 of Appendix B.

RECOMMENDATION:

prepare a formal contingency plan for the Threeville field office.

2.4 TORNADOES

HEADQUARTERS, FOURVILLE AND TOURVILLE

It has been determined by the examination of various maps that there was one occurrence of a tornado in both of the one degree square areas surrounding the Office of Employment Security Capitaltown headquarters offices and the Fourville and Twoville field offices over a thirteen year period. Each one degree square encompasses approximately forty-nine hundred square miles.

The annual frequency estimate is then derived by dividing the number of square miles in the one degree square area (4900) into

the approximate number of tornadoes occurring in that are in any one year (1/13). The resultant annual frequency estimate for tornadoes which specifically impact the Office of Employment Security headquarters facilities and the Twoville and Fourville filed offices is calculated to be (1/13)/4900 which is equal to .00002.

The AFE is so small that the risk of loss due to tornadoes is negligible.

THREEVILLE

It has been determined from various maps that there were four tornadoes in the one degree square area surrounding the Threeville field office during a thirteen year period. This one degree square encompasses approximately forty-nine hundred square miles.

The annual frequency estimate is the derived by dividing the number of square miles in a one degree square area (4900) into the approximate number of tornadoes occurring in that area in any one year (4/13). The resultant annual frequency estimate for tornadoes which specifically impact the Office of Unemployment Security's Threeville field office is calculated as (4/13)/4900 which is equal to .00006.

This AFE is so small that the risk of a serious loss is negligible.

2.5 POWER OUTAGES

Although there are approximately two or three power outages per year in all SOES facilities, there is no significant impact on processing because there is no overtime associated with downtime up to two hours and none of the outages have lasted that long.

There is no significant risk of loss due to power outages.

2.6 A/C OR HEATING FAILURE

There have been no cases of State Office of Employment Security employees being sent home because of the lack of air conditioning or heat.

A preventive maintenance program is being followed to minimize the possibility of a breakdown in the electrical and mechanical systems.

There is an air conditioning service on call to handle any breakdown twenty-four hours a day, seven days a week.

The existence of a preventive maintenance program and the availability of the on-call air conditioning service makes the risk negligible.

2.7 THEFT/ROBBERY/UNAUTHORIZED ACCESS

HEADQUARTERS

Due to the location of the Office of Employment Security headquarters buildings in an area containing some popular tourist attractions, the potential for unauthorized access is greatly increased.

FINDINGS 2.7-1:

Headquarters offices are susceptible to unauthorized access.

RELATED CONTROL STANDARD 5137 (N)(7):

During normal working hours, access to the Unemployment Insurance Bureau claims work area is generally to be restricted to company employees. The presence of all visitors is to be controlled.

DISCUSSION:

When we passed the loading dock guard station at 123 Main Street on various occasions, the guard was absent. On further inspection we observed the guard standing near 1st Street, which is located one-half black down the street from the loading dock.

RISK ANALYSIS:

We feel that 123 Main Street is susceptible to unauthorized entry through the loading dock door due to inadequate monitoring by the guard force.

Losses to SOES could occur by theft, fraud or vandalism. Blank checks as well as signed checks ready for mailing are stored in rooms whose walls do not extend to the true ceiling. CRT terminals which can access restricted files such as the Master Employer File are located in the building. Office spaces for Unemployment Insurance Bureau management personnel are also located in the building and could be vandalized.

The risk of fraud and abuse through manipulation of computerized Unemployment Insurance Bureau data is evaluated in Findings 3.2.1.1.2-1 and 3.3-1. The risk of theft is treated in Finding 3.5.1-1.

In this finding we will account for the threat of vandalism and other destructive acts. Although intruders could probably gain access to the headquarters buildings with little difficulty, there are in fact no cases of vandalism on record. For that reason we select an AFE of 1 from the low end of the scale.

The loss potential, considering only Unemployment Insurance Bureau assets, is set at $100K. this includes losses due not only to the physical destruction of tangible assets but also to the damage done to paper records and data contained on other physical media.

The ALE is $100K x 1 = $100K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The suggested safeguard is to enforce existing guard procedures more strictly. The cost should not exceed 1 hour per day of staff time by a guard supervisor at a salary level of $18K per year including overhead. This amounts to (1/8) x $18K/yr = $2.3K per year.

The ALE would be reduced by 95% to $5K.

The savings will be ($!00K - $5K) - $2.3K = $93K.

See the risk analysis worksheets in Section B.4 of Appendix B.

RECOMMENDATION:

Monitor the performance of the guard force and demand compliance with established procedures.

FINDING 2.7-2:

The wearing of badges at 456 Main Street is not enforced.

RELATED CONTROL STANDARD 5137(N)(7):

During normal working hours, access to Unemployment Insurance Bureau Claims work areas is generally to be restricted to Bureau employees. The presence of all visitors is to be controlled.

DISCUSSION:

Employees at 456 Main Street do not all wear their SOES badges. Unescorted visitors could pocket their badges and be taken for employees.

RISK ANALYSIS:

Because badges are not generally worn, an intruder or a bona fide visitor could masquerade as a SOES employee and move freely through the building. The fact that the upper floors are not currently occupied would allow such a person to hide until after normal business hours. He could then commit destructive acts or steal assets such as benefit checks or office equipment and depart undetected.

This problem is closely related to Finding 3.11.2-1. The risk analysis is not repeated here because we feel that this would tend to make a single access control problem with several facets appear to be a number of independent problems. In addition it would unreasonably inflate the loss expectancy.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION:

Enforce the wearing of badges at 456 Main Street.

999 BACK STREET

The State Supply Warehouse is surrounded by streets on three sides and a parking lot on the fourth side. The walls are sheer from the ground to the rooftop level above the fourth floor. A fire escape ladder extends from the roof to ground level.

FINDING 2.7-3:

The State Supply Warehouse is susceptible to unauthorized access.

RELATED CONTROL STANDARD 5137(N)(1):

All Unemployment Insurance Bureau assets and related operations must be secured against unauthorized access.

DISCUSSION:

The State Supply Warehouse building has a guard at the front entrance who checks the ID of persons entering. If an intruder wanted to gain access to the warehouse, he could go to the side of the building and climb up the fire escape ladder to the roof. Once on the roof, the intruder could enter the warehouse by breaking the skylight window.

We also discovered that the motor for the elevator is housed in a structure on top of the roof. The elevator motor is protected by an easily breached wire mesh screen. An intruder could easily bypass the screen and gain entry to the warehouse by climbing down the elevator shaft and out onto one of the floors.

By entering the third floor, the intruder could set the record storage area on fire, destroying the Unemployment Insurance Bureau records and possibly causing damage to the warehouse building.

RISK ANALYSIS:

There is no good reason why individuals would want to enter or vandalize the warehouse facility except for retaliatory purposes against the Office of Employment Security organization. This is because of the minimal amount of valuable assets contained in the building and because there are many other warehouse facilities in the same area which could also be looted or damaged.

In conclusion, there would be little motivation for breaking into the Sate Supply Warehouse and consequently the AFE for either unauthorized access or vandalism to the facility would be very low.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION

FOURVILLE AND TWOVILLE

The Fourville Field office is a single story masonry structure occupying one-quarter of a square block. The building is also occupied by a restaurant and real estate agency.

A restaurant occupies one third of the building in which the

Office of Employment Security Office at Twoville is located.

Because there are other operating business in the immediate vicinity of both field offices, their employees and customers move about the vicinity of the offices, increasing the potential for unauthorized access. However, the buildings are equipped with door alarms and motion detectors which minimize the risk of unauthorized entry during non-business hours.

THREEVILLE

Because other businesses occupy part of the building in which the Office of Employment Security office is housed, their employees and customers move about the vicinity of the office increasing the potential for unauthorized access.

FINDING 2.7-4:

The Threeville Field Office is susceptible to unauthorized access.

RELATED CONTROL STANDARD 5137(N)(1):

All Unemployment Insurance Bureau assets and related operations must be secured against unauthorized access.

DISCUSSION:

There is a gap between the top of the rear exit door and the doorframe. A normally closed magnetically controlled switch is attached to the doorframe within reach of the gap. A magnet is attached t the door in such a way that when the door is closed, the magnet touches the switch and causes it to open. If an intruder were to open the door, the magnet would move away from the switch; the switch would then close and set off the alarm. The intruder could place his own magnet near the switch through the gap at the top of the door and then open the door without closing the switch and setting off the alarm.

The photoelectric beam detectors are not adequate for protection because no matter how the beam is adjusted, it can be by passed either by jumping over it or by crawling under it to gain entry into the field office.

After we learned that established procedures required that the door leading from the parking lot into the training room be locked to prevent unauthorized access, we checked it and discovered it to

be unlocked.

The door leading form the rear parking lot into the Threeville filed office record storage area is made of a flexible metal material which is unsturdy and therefore easily penetrable with minimal effort.

RISK ANALYSIS:

Whereas Fourville and Twoville are relatively well protected from unauthorized access, Threeville is vulnerable because its alarms can all be bypassed easily and because the reception area is poorly monitored during the early morning and the later afternoon. (See Finding 3.2.1.3-1.)

The lease cost for EDP equipment in the Threeville field office was $17,866 for the month of December, 1982. If this equipment were stolen or destroyed, SOES would be liable for these charges for the remaining 3 years of the lease. This would amount to 36 mos x $17,866 = $643K.

The AFE of 5 is larger than for other sites because of the ease of unauthorized access.

THE ALE is then $643K x 5 = $3.2M. This is a worst case figure which reflects what might happen if the access control vulnerability were discovered and exploited by a criminal and SOES failed to take any corrective action. Thieves could then loot the office over and over again.

Actually, SOES would implement more effective controls after the first serious theft in order to eliminate the problem.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

A number of steps should be taken. The beam alarms should be replaced with motion detectors. The seven soft-metal warehouse doors, covered on the inside with sheetrock, should be removed and the outside wall bricked up. The rear exit door with the gap at th top should be replaced with a much sturdier well-fitted door. All outside doors except the main entrance should be locked and alarmed during the day. The main entrance door should be equipped with a signaling device which would sound when the door is opened from the outside.

The cost of all these modification should not exceed $20K.

The ALE will be effectively reduced to $0.

The 5-year savings will be ($3.2M - $0) x 3.79 - $20K = $12M.

See the risk analysis worksheets in Section B.5 of Appendix B.

RECOMMENDATION:

Repair the gap in the rear exit door. replace the photoelectric beam detectors with motion detectors.

FOURVILLE, TWOVILLE AND THREEVILLE

FINDING 2.7-5:

The custodial service at the field offices perform their duties after hours and are not supervised by SOES personnel.

RELATED CONTROL STANDARD 5137(N)(11):

Limit the presence of cleaning and maintenance personnel tot he period when there are some regular facility employees on duty.

DISCUSSION:

Custodial services in the Fourville, Twoville and Threeville field offices are performed outside of regular working hours and without the supervision of Office of Employment Security personnel.

This would not be a vulnerability if sensitive records and valuable equipment in the building were properly protected.

However, many sensitive files are stored in unlocked cabinets in open areas and valuable items of relatively portable equipment are not secured.

In the absence of supervision, custodial employees could easily commit dishonest or destructive acts. Although these personnel are bonded, it is usually necessary that a crime be proven in court before the bond can be collected. In addition, there is valuable information in the field offices which could be stolen by copying or photography and thus never missed.

RISK ANALYSIS:

It is unlikely that bonded custodial personnel would vandalize the

field offices. It is also unlikely that they would commit obviously detectable crimes such as the theft of tangible resources. Bonded personnel would be more apt to commit "undetectable" crimes such as copying the wage record file (with a camera, for example).

The loss potential, which is independent of the nature of the threat agent, is set at $100K.

Because of the bonding and the fact that no problems of consequence have been associated with the custodial serves, a low AFE of .5 is chosen.

The ALE is then $100K x .5 = $50K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

Several safeguards are possible. Janitorial services could be performed during normal business hours with a little inconvenience to SOES personnel. The services could be performed at night with a SOES supervisor present or they could be performed by SOES employees instead of contractor personnel.

Each of these three safeguards would result in the monitoring of custodial personnel by SOES employees in accordance with generally accepted practices.

The cheapest of the three solutions would be to use existing contractor personnel during normal business hours. There would be no additional direct cost. In fact, wage rates might be lower for daytime services.

One indirect cost would be due to brief interruptions of the office staff by the janitors. This should not amount to more than 2 minutes per day per person. For 320 field office employees, using an average salary of $6.50 per hour and 25% overhead, the cost of .2 minutes per day lost time would be 2 min/day x 1/60 hrs/min x 320 staff x $6.50/hr x 1.25 overhead x 5 days/wk x 52 wks/yr = $23K.

The ALE will be reduced by 90% to $5K.

The savings will be ($50K - $5K) - $23K = $22K per year.

See the risk analysis worksheets in Section B.6 of Appendix B.

RECOMMENDATION:

Have the custodial services perform their duties during normal business hours.

CHAPTER 3

SPECIFIC ISSUES

3.1 INTRODUCTION

This chapter is similar in format to Chapter 2. Each section contains a *BACKGROUND AND INTRODUCTION* followed by a series of one or more findings. For each finding there are paragraphs entitled *FINDING, RELATED CONTROL STANDARD, DISCUSSION, RISK ANALYSIS, SUGGESTED SAFEGUARDS AND COST BENEFIT ANALYSIS, and RECOMMENDATION*. The contents of these paragraphs are as outline at the beginning of Chapter 2.

The sections of this chapter are based on the organizational structure of SOES. Each functional group, department, division, branch and section which performs functions in support of SOES Unemployment Insurance Bureau Operations was examined in the risk analysis. Only those organizational elements which could have a security or integrity related impact on Unemployment Insurance Bureau Operations are specifically included in this chapter.

Each group of organizational elements at one level appears after the element at the next higher level. Thus Employer Audit Unit and Program Integrity appear after Employer Audit and Review.

3.2 SOES, UNEMPLOYMENT INSURANCE BUREAU

BACKGROUND AND INTRODUCTION:

The SOES Unemployment Insurance Bureau Department is responsible for all aspects of processing Unemployment Insurance Bureau insurance claims in the state. The Department uses field offices in Twoville, Threeville and Fourville in addition to its headquarters staff in Capitaltown to accomplish its work. Data processing services are provided by Turnkey Systems Inc., an Unemployment Insurance Bureau contractor.

3.2.1 UNEMPLOYMENT INSURANCE BUREAU CLAIMS OPERATIONS

BACKGROUND AND INTRODUCTION

This department is responsible for all aspects of claims processing including direct data entry, adjustments and overpayment processing, correspondence and telephone, cash disposition accounting, eligibility checking of claimants and benefit charging of employers. The work is done primarily in field offices.

3.2.1.1 FOURVILLE FIELD OFFICE

BACKGROUND AND INTRODUCTION:

The Fourville field office is currently responsible for Adjustments and Overpayments Processing and the direct data entry of claims involving major employers. Eventually, Fourville is to be responsible for all aspects of claims processing.

FINDING 3.2.1.1-1:

The Wage record file is unprotected.

RELATED CONTROL STANDARD 5137(N)(19):

Provide for the secure storage of all media containing sensitive data when it is not in use.

DISCUSSION:

The Wage record file contains data on all persons in the SOES service area who are potential Unemployment Insurance Bureau claimants. Printed versions of portions of the file are kept in open storage. It would be of significant commercial value to any firm marketing products or services generally useful to individuals in specific income brackets and is therefore subject to misappropriation. It must be given proper protection under the State Privacy Act of 1974.

The problem exists at both the Twoville and Fourville field offices. The numbers used in the analyses below reflect both offices. The finding but not the analysis is repeated in Section 3.2.1.2 for cross-reference purposes.

RISK ANALYSIS:

The Wage Record file is most susceptible to theft by a SOES employee since it is stored in an area normally accessible only to employees. However, the Twoville and Fourville field offices are susceptible to unauthorized access in the early morning and late afternoon (see Section 2.7).

The known range of AFEs for theft from businesses is 1 to 50. Considering the ease of theft in this case, as well as the fact that there has been no previous record of thefts, we have selected an AFE of 5.

Although the Wage Record file has no intrinsic value and can easily be replaced, there is a potential loss to SOES through a State Privacy Act lawsuit filed by a Unemployment Insurance Bureau claimant who will argue that SOES was negligent in protecting the sensitive information entrusted to it.

A study of known State Privacy Act cases shows that the likelihood of a lawsuit is .0001 to .01 per year. Because of the ease of the theft and the large volume of privacy data involved and because of the fact that SOES has and no previous lawsuits of this nature, we have selected an AFE or .001, in the middle of the range. The cost to SOES might be as much as $20K for legal fees and $100K in compensatory and punitive awards.

The ALE is then $120L x 5 x .001 = $600

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The suggested safeguard is to control access to the Wage record file during the day and store it in a locked filing cabinet at other times.

The cost of this safeguard is estimated to be 15 minutes of staff time per day or 52 x 5 x 1/4 = 65 hours per year. Using the wage rate for a general clerk of $4.75 per hour and an overhead rate of 25%, the total cost per year would be 65 hours x $475 per hour x 1.25 = $390.

The safeguard would be expected to reduce the ALE by 90% to $60.

The expected yearly savings would then be equal to the ALE reduction minus the safeguard cost or ($600 - $60) - $390 = $150.

See the risk analysis worksheets in section B.7 of Appendix B.

RECOMMENDATION:

Provide secure storage for the Wage Record file at the Twoville and Fourville field offices.

FINDING 3.2.1.1-2:

The outside entrance to the Fourville field office is unmonitored during the early morning and late afternoon hours.

RELATED CONTROL STANDARD 5137(N)(2):

Control must also be maintained in other Unemployment Insurance Bureau work areas over the presence of visitors, and the presence of employees after normal working hours.

DISCUSSION:

The reception area of the Fourville field office is separated from the main work areas. Due to flextime work schedules, this area is sometimes unstaffed during the early morning and late afternoon. It would be simple for a person to walk in and conceal himself or to steal a typewriter or other item of equipment from the reception area during these times.

RISK ANALYSIS:

It would be a relatively simple matter for a person to slip into the reception area unobserved and conceal himself until the SOES staff departed. The person could then disable the door open sensors attached to the burglar alarm and remove a large quantity of expensive office equipment. The monthly lease cost of this equipment which includes approximately 82 CRTs, 60 MDTs, a line printer, a micrographics printer, 2 microfiche readers, and 2 16mm printers is about $10K.

The range of AFEs for theft (from Finding 3.2.1.
1-1) is 1 to 50. Because we are now considering the theft of bulky equipment which would require some time to move and truck to haul away, we will choose an AFE well below the top of the range. Because of the ease of initial access to the facility, the AFE must be above the bottom of the range. However, the need to by pass the motion detectors which operate during non-business hours complicates the situation and tends to hold the AFE close to the bottom of the range. We thus select an AFE of 2.

If the leased ADP equipment were stolen or damaged, SOES would be responsible for the payments for the remainder of the lease period. This would be approximately 3 years and would amount to $360K.

The ALE is then $360K x 2 = $720K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The suggested safeguard is either to ensure continuous staffing of the reception area or to install a signaling device which will sound when the entrance door is opened from the outside.

Continuous staffing of the reception area is estimated to cost at least one additional hour of staff time per day. Using the wage rate for a general clerk of $4.75 per hour and the overhead rate of 25% this would be 52 wks x 5 days/wk 1 hr/day x $4.75/hour x 1.25 = $1,550 per year.

The cost of installing a signaling device on the entrance door would be a one-time charge of not more than $300. this is clearly the more cost-effective safeguard.

The ALE would be reduced to $0 by this safeguard.

the savings to be expected over the standard 5-year amortization period is then 3.79 x ($720K - $0) - $300 = $2.7M.

see the risk analysis worksheets in Section B.8 of Appendix B.

RECOMMENDATION:

Ensure that the reception area is staffed at all times when the main entrance door is unlocked. Alternatively, install a bell or other signaling device which will sound when the door is opened from the outside.

3.2.1.1.1. EMPLOYER'S CHARGE

BACKGROUND AND INTRODUCTION:

The determination of charges to employers is carries out by this unit, This unit also verifies the correctness of wage records in disputed cases.

We found no problems with the practices and procedures of this

unit.

3.2.1.1.2 ADJUSTMENTS AND OVERPAYMENTS

BACKGROUND AND INTRODUCTION:

The Fourville filed office currently performs all adjustments and overpayments processing. This is done by three units operating under a general supervisor.

FINDING 3.2.1.1.2-1:

It is possible for an Adjustments and Overpayments processor to reactivate and pay a claim or to make an adjustment to a claim in a fraudulent manner.

RELATED CONTROL STANDARD 5137(C):

Organizations must employ effective measures, consistent with their operational environment, to limit the potential for unassisted fraud.

DISCUSSION:

It is the function of the adjustments and overpayments processors to make decisions to pay or deny claims in situations where human evaluation of the circumstances is required. Although the processors are relied upon to apply very detailed guidelines in carrying out this function, they could easily abuse their authority and handle some claims in a fraudulent manner. The odds of being caught in a quality control audit would be non-zero but small.

RISK ANALYSIS:

Although there has been no history of violation of trust by SOES employees in the field offices, this is at least partially due to the impossibility of carrying out a second party review of all claims processing actions.

The range of AFEs for fraud and abuse nationally is .006 to .09.

There are approximately 10K adjustment/overpayment actions per day or 10K x 5 x52 = 2.6M per year. The standard for suspense processing is between 61 and 69 claims per hour depending on the location. Using 65 as an average, about 16 processors are required to handle the workload. These processors are normally

audited at the rate of 50 to 100 claims per month or an average of 75 x 12 = 900 per year.

The likelihood of a single fraudulently processed claim being audited is thus about (900 x 16) / 2.6M = 15.4K / 2.6M = .006. This means that a processor would risk only 6 chances in 1,000 of having a fraudulent claim reviewed by a second party.

Because of the low risk involved, we select the AFE to be the top of the range or .09.

FBI statistics indicate that the average computer crime nets $500,000 for the perpetrator. This figure seems high for the present situation and a large number of fraudulent transactions would be required to reach 1t. A loss of $100K per year would be a more reasonable upper bound on the amount that could be diverted through fraudulent adjustments/overpayments processing.

The ALE is then $100 x .09 = $9K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The suggested safeguard is to apply the principle of separation of duties. In order to convert Unemployment Insurance Bureau funds to their own use, processors would have the change the payee address associated with the claim. Such actions should be isolated as privileged transactions and assigned to special processors who are not authorized to carry out other types of transactions.

This safeguard would cost about 3 staff-months for procedure redesign and another 3 staff-months for modifications to CUIS. We use an annual salary of $30K and 100% overhead for programming modifications and a grade 34 salary plus 25% overhead for procedure redesign. This amounts to (1/4 x $23,678 x 1.25) + (1/4 x $30K x 2.0) = $22K.

The ALE reduction would be about 90% yielding a reduced ALE of $900.

The savings would be ($9K - $900) x 3.79 - $22K = $9K.

See the risk analysis worksheets in Section B.9 of Appendix B.

RECOMMENDATION:

Apply separation of duties between adjustments and overpayments processing and other aspects of claims processing.

3.2.1.1.3 ADJUDICATION

BACKGROUND AND INTRODUCTION:

This unit is responsible for ensuring that Unemployment Insurance Bureau claimants are eligible and that employers are properly registered within the Unemployment Insurance Bureau program.

We found no problems with the practices and procedures of this unit.

3.2.1.1.4 CLERICAL SUPPORT

BACKGROUND AND INTRODUCTION:

This unit provides administrative support to the Fourville field office as well as support services for the Unemployment Insurance Bureau claims processing operation. This includes management of general office services such as copiers, vending machines, janitorial services, etc.; management of paper and microfilm records; and supervision of employee time and performance accounting.

We found no problem with the practices and procedures of this unit.

3.2.1.1.5 AUDITING/TRAINING

BACKGROUND AND INTRODUCTION

This unit is responsible for the quality control auditing of claims processors as well as the functional training of newly hired claims processors. The unit reports directly to the field office manager.

We found no problems with the practices and procedures of this unit.

3.2.1.1.6 TSI SUPPORT

BACKGROUND AND INTRODUCTION:

TSI provides a trainee systems analyst at each Unemployment Insurance Bureau field office to support claims processors when

software problems or local hardware problems arise.

We found no problems with the practices and procedures of this analyst.

3.2.1.1.7 PERSONNEL

BACKGROUND AND INTRODUCTION:

This unit, currently consisting of one person, provides all personnel services for the Twoville and Fourville field offices. The unit reports to Personnel at SOES HQ in Capitaltown. Roughly half of the time is spent at Fourville and half at Twoville.

3.2.1.2 TWOVILLE FIELD OFFICE

BACKGROUND AND INTRODUCTION:

This field office is responsible for correspondence processing, cash disposition accounting, telephone inquiries and direct data entry of claims.

FINDING 3.2.1.2-1

The Wage record file is unprotected.

RELATED CONTROL STANDARD 5137(N)(19):

Provide for the secure storage of all media containing sensitive data when it is not in use.

DISCUSSION

This problem is discussed under Finding 3.2.1.1-1. The numbers used in the Risk Analysis and Cost-Benefit Analysis paragraphs of that finding cover both the Twoville and the Fourvile field offices. Consequently, these paragraphs are omitted hers.

RECOMMENDATION:

Provide secure storage for the Wage Record file at the Twoville and Fourville field offices.

FINDING 3.2.1.2-2:

Outside doors to the Twoville field office (other than the main

entrance are unalarmed during business hours.

RELATED CONTROL STANDARD 5137(N)(2):

Control must also be maintained in other Unemployment Insurance Bureau work areas over the presence of employees after normal working hours.

DISCUSSION:

Although there is a policy that doors other than the main entrance door not be used by employees exiting the building, there is no practical means of enforcing the policy.

Because these doors can be used during the day, there is a possibility that they will not be closed properly and that unauthorized access to the facility will be made easier.

RISK ANALYSIS:

Although these unalarmed doors represent a security deficiency, it would not be a straightforward matter to take advantage of the situation. It would be possible for a person to wait for an opportunity to gain access through these doors, but the time required and the uncertainty of success would reduce the AFE to the lower end of th scale.

The range of AFEs for theft and unauthorized access is 1 to 50. Consequently we choose 1 as the AFE.

There are approximately 118 CRTs and 60 MDTs in the Twoville field office with a lease cost of about $14K per month or $170K per year.

With 3 years of lease payments remaining, the ALE for theft of this equipment is then 3 x $170 x 1 = $510K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The suggested safeguard is to install deadbolt locks on the doors in question and issue keys to the employees who have an official need for them.

This safeguard would have a one-time cost of not more than $300 and would reduce the ALE by 100% from $510K to $0.

The savings would be 3.79 x (150K - $0) - $300 = $1.9M.

See the risk analysis worksheets in Section B.10 of Appendix B.

RECOMMENDATION:

Install deadbolt locks on all but the main entrance door. Issue keys to those who must use the doors in the conduct of their official duties.

FINDING 3.2.1.2-3:

Dry chemical fire extinguishers are provided for work areas in which CRT terminals are located.

RELATED CONTROL STANDARD 5137 J(1)(C):

Avoid the use of carbon dioxide area extinguishing systems since they present a significant safety hazard.

DISCUSSION:

Dry chemical fire extinguishing agents will damage electronic circuitry beyond repair. Other agents such as halon are equally effective fire suppressants but will not cause any damage to circuitry.

RISK ANALYSIS:

Use of dry chemical extinguishers would be detrimental only in those fire situations in which electronic equipment would be saved if non-destructive extinguishing agents were used. This would include only small area fires detected soon after starting and would involve at most 4 to 6 CRTs.

The AFE for a small fire occurring during business hours is .1. This number results from data collected by State fire inspection authorities and from national data.

The lease cost of 6 CRTs is about $750 per month or $27K for the 3 years remaining in the agreement. This value would be totally lost if the CRTs were sprayed with dry chemicals. There would be no loss if halon were used.

The ALE is thus $27K x .1 = $2.7K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

Replace the dry chemical extinguishers with halon extinguishers. The cost will be about $200 each. Six extinguishers would then cost $1,200.

The ALE reduction would be 100%. The 5-year savings would then be the amortized value oft he 5-year loss reduction less the one-time cost of the safeguard or 3.79 x $2,7K - $1,200 = $10K.

See the risk analysis worksheets in Section B.11 of Appendix B.

RECOMMENDATION:

Replace the dry chemical extinguishers with halon extinguishers.

FINDING 3.2.1.2-4:

Documents describing restricted access software are not given special protection in the Twoville field office.

RELATED CONTROL STANDARD 5137(N)(1):

All Unemployment Insurance Bureau assets and related operations must be secured against unauthorized access; this includes sensitive data in transit within the organization.

DISCUSSION

The same documents which are kept under lock and key in the Fourville filed office are not similarly protected in the Twoville filed office. This reflects a lack of central control over security procedures. It also represents a failure to restrict information which would give unauthorized persons the ability to access restricted software and data.

RISK ANALYSIS

The effect of this finding is to make it easier for unauthorized persons to access restricted software. This software includes WRK-PLN and PERF-MON which are not directly concerned with claims processing but rather with workload planning and employee performance. Unauthorized access would not result in an illegal diversion of funds. It would possible lead to intra-office rivalries and ill feelings which would decrease the efficiency of the staff.

Using an average salary rate for claims processors of $5.50 per

hour, an overhead rate of 25% and a staff size of 105, the annual claims processing staff cost is 105 staff x 1.25 overhead x 52 wks/yr x 5 days/wk x 8 hrs/day x $5.50/hr = $1.5M.

A cut in efficiency of only 5% due to staff infighting would then result in a loss of $1.5M x .05 = $75K per year, the ALE.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

Provide proper protection for documents describing restricted software. Although protecting the software by means of passwords or user security profiles would be a more effective solution, it would also be more costly.

The existing documents should be stored in locked desks or cabinets until it becomes cost-effective to implement password or user profile protection.

The cost of establishing and enforcing secure storage procedures should not exceed 15 minutes per day of supervisor time.

This would amount to 1/4 hr/day x 52 wks/yr x 5 days/wk x 1.25 overhead x $7.35/hr = $600 per year.

This safeguard should reduce the ALE to $0 because the target of the threat is not sufficiently attractive for anyone to use much effort in gaining access to it.

The savings would then be ($75K - $0) - $600 = $74 per year.

See the risk analysis worksheets in Section B.12 of Appendix B.

RECOMMENDATION

Access to restricted software should be controlled through passwords or user security profiles, not through the secrecy of operating procedures. In the present situation, the restricted documents should be stored in locked desks or cabinets.

3.2.1.2.1 DATA ENTRY

BACKGROUND AND INTRODUCTION:

The data entry function is organized into three operating units and one auditing unit, all reporting to a general supervisor.

We found no problems with the practices and procedures of the data entry units. Findings related to the auditing unit are discussed in Section 3.2.1.2.5.

3.2.1.2.2 CORRESPONDENCE

BACKGROUND AND INTRODUCTION

Correspondence processing comprises all activities involved in the handling of written queries from Unemployment Insurance Bureau employers, claimants and other interested parties. An online subsystem of CUIS is used to generate automated responses to such inquiries.

There are two operating units, a control/microdata unit (which also services the cash disposition and data entry groups) and an auditing unit, all under a general supervisor.

We found no problems with the practices and procedures of the Correspondence units or the control/microdata unit. Findings relating to the auditing unit are discussed in Section 3.2.1.2.5.

FINDING 3.2.1.2.2-1:

Correspondence processors can divert claim payments from their intended recipients in a variety of ways.

RELATED CONTROL STANDARD 5137(C)(1):

Organizations must employ effective measures, consistent with their operational environment, to limit the potential for unassisted fraud. For example, a computer console operator should not be allowed to write programs and introduce them into the system, or to introduce any programs not authorized by someone responsible for the internal control, such as the tape librarian. Further examples of the duties that should not be assigned the same employee at the same time are scheduling, operating, programming, storage, and library functions; nor should employees be allowed to perform unassigned duties that might increase the range of their activities.

DISCUSSION:

The primary mechanism is the fraudulent address change. The capability also exists for processors to restore the correct address after payment has been made.

There is a risk of being caught in a quality control audit but the risk is small.

RISK ANALYSIS:

This finding is essentially similar to Finding 3.2.1.1.2-1. Because all claims processors have access to all aspects of claims processing, it would be repetitive to assess separately potential losses due to fraud by correspondence processors and adjustments and overpayments processors.

Consequently, the reader is referred to Finding 3.2.1.1.2-1 for risk analysis calculations.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION:

Determine patterns of claims processing transactions which would be carried out when fraud was being attempted. Flag for special review al claims to which these patterns apply.

3.2.1.2.3 CASH DISPOSITION

BACKGROUND AND INTRODUCTION:

The general supervisor of cash disposition also oversees the Telephones Unit and an Auditing Unit. The Cash Disposition Unit assists in Unemployment Insurance Bureau benefit fund accounting by using an online CUIS subsystem to enter data related to returned benefit payment checks, stale-dated check, recouped overpayments, etc.

No cash or checks are handled by this office except in rare instances when they are sent to Twoville by mistake instead of to Capitaltown.

FINDING 3.2.1.2.3-1:

Passwords controlling access to CUIS Cash Disposition functions are not changed when employees who know them terminate their employment.

RELATED CONTROL STANDARD 5137(J)(13):

prompt action must be taken to delete an employee's personal identification number or other identifier from the system authorization list or table when the employee no longer has the authority to access a system (e.g., after changing function or leaving the organization.)

DISCUSSION

This problem is discussed more generally in Finding 3.3-5 below. Terminating employees could misuse their knowledge either for personal gain or to get revenge for their perceived mistreatment by SOES.

The Risk Analysis and Cost-Benefit Analysis paragraphs are omitted here because this problem is covered in the analysis of Finding 3.3-1.

RECOMMENDATION:

All access control keys (both logical can physical) should be returned to SOES or rendered unusable upon th termination of employees who possess them.

FINDING 3.2.1.2.3-2:

Passwords controlling access to CUIS Cash Disposition functions are sometimes written down by the clerks entrusted with them.

RELATED CONTROL STANDARD 5137(J)(12):

Passwords must not be displayed on the video display terminals or hardcopy devices. Ensure that the computer operators, acting without authority, are not able to display user programs or circumvent security mechanisms.

DISCUSSION

When written down, passwords become much more accessible to unauthorized parties. A knowledgeable person would assume that the password was written down and search the work area of the employee who regularly uses it. Typical places to look would include calendar pads, blotters and little slips of paper.

RISK ANALYSIS:

This is another finding relating to a lack of proper password

management. The risk analysis and cost-benefit analysis of this issue are contained in Finding 3.3-1.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION:

Establish and enforce a policy that passwords are not to be written down.

FINDING 3.2.1.2.3-3:

There is no effective control over mail which may be addressed to specific field office employees and which may contain checks made out to those employees.

RELATED CONTROL STANDARD 5137(K)(5):

During non-working hours, Unemployment Insurance Bureau-related work materials must be stored in a secure area, such as an entire floor or room. In the event that this access control can be achieved by securing the entire building, it is not necessary to apply restrictive measures to individual locations within the building.

DISCUSSION:

Occasionally an Unemployment Insurance Bureau claimant will attempt to reimburse SOES for an overpayment made on a claim by writing a check to a specific SOES employee. In the absence of controls, the employee can cash the check and pocket the money. He could do this with relative impunity when the overpaid amount is less than $50 because recoupment of such small amounts is not pursued beyond the mailing of a single letter requesting repayment.

RISK ANALYSIS:

An enterprising cash disposition clerk could attempt to increase the likelihood that checks would be addressed to and/or made out to him. He could then cash all such checks he received.

In the worst case a clerk might manage to receive 100 checks per year worth about $100 each for a total of $10K.

As this is not a difficult thing to do, we choose the AFE for this form of fraud and abuse from the high end of the range, .09.

The ALE is then $10K x .09 = $900.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

By requiring all staff members to open personally addressed mail received at the office in the presence of a supervisor, the ALE will be reduced by 95%.

The reduced ALE will then be .05 x $900 = $45.

The safeguard cost will be essentially zero. The resulting savings is then $860 per year.

See the risk analysis worksheets in Section B.13 of Appendix B.

RECOMMENDATION

Require that mail addressed to individual employees be opened by mailroom personnel or in the presence of a second party. Require also that employees not intentionally direct personal mail to the SOES address.

3.2.1.2.4 TELEPHONES

BACKGROUND AND INTRODUCTION:

The Telephone unit operates under the same general supervisor as the Cash Disposition Unit. The unit responds to telephone inquiries related to Unemployment Insurance Bureau claims. A Rolm Automated Call Distribution (ACD) System detects incoming calls, routes them to available unit personnel and places excess calls on hold. The ACD System has a control keyboard and a CRT display. It reports statistics on its operations. There are 12 eastern state WATS lines, 4 western state WATS lines and 5 local lines.

FINDING 3.2.1.2.4-1:

Address changes are accepted from Unemployment Insurance Bureau claimants over the telephone.

RELATED CONTROL STANDARD 5137(N)(13):

Make sure of the identity of outside personnel into whose

possession Unemployment Insurance Bureau data are to be release. Special attention should be given to release of personnel information by telephone either within the organization or to the people outside.

DISCUSSION:

The address associated with the payee of a claim constitutes sensitive information as it specifies where potentially large amounts of money will be sent. Persons having the ability to manipulate such address information in effect have the ability to control the disbursement of Unemployment Insurance Bureau benefit funds.

To change a claimant's address by telephone, a caller must know only the claimant's name, address and registration number, information which is easily acquired.

A clever swindler would find a way to get the necessary information for a relatively large claim and change the address to one not associated with him personally but which he could monitor for delivery of the benefit check. When the check arrived, the swindler would steal it form the mailbox unbeknownst to the owners and cash it.

RISK ANALYSIS:

to make such an operation worthwhile, a swindler would probably target larger claims only. He could get the necessary information by taking a janitorial job in a private employment service and using his access to the facility to gain access to applicant records.

With careful planning, the swindler might divert 1,000 or more checks worth $100,000 total over a short period of time. The operation would have to be abandoned by the time the intended payees reported non-receipt of their checks because the resulting investigation would soon focus on the private employment service itself.

The same type of operation might be carried out over a longer period of time at multiple facilities. In this case the swindler would divert only one check form each facility in order to keep his modus operandi secret.

The AFE for fraud and abuse of .006 applies. The low end of the

scale is used because of the complicated nature of the fraudulent activity.

The ALE is $100K x .006 = $600.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

One suggested safeguard is to require change of address request to be in writing over the signature of the claimant. This would foil casual swindlers not willing to spend a lot of time and energy on their attempted fraudulent activity, but it would not deter the serious con artist described above who would have access not only to the claimant's personal data but also to copies of his signature.

A more effective safeguard would be to issue each claimant a secret password or number to be used as an authorizing code for address changes and other transactions of import. Such a mechanism is already being used by banks, especially those with automated teller terminals.

This latter safeguard should reduce the ALE by 95% to $30.

The cost of the safeguard is estimated at 3 staff-months for programming modifications to CUIS to generate, use and store the secret codes, plus 1 staff-month of administrative time and $10K for notification of the claimant. We have used $30K salary and 100% overhead for programming changes and a grad 30 salary and 25% overhead for administrative time. This amounts to (1/4 x $30K x 2.0 + 1/12 x $19,947 x 1.25) + $10K = $27K.

This safeguard is clearly not cost-effective. A less expensive approach would be to record several items of information known only to each claimant and ask the claimant to supply one or more of these items when he requests an address change. The cost of this safeguard would be about one man-week of programming at an annual rate of $30K and 100% overhead or $30K x 2.0 x (1/52) = $1.2K.

The ALE will be reduced by 95% to $30.

The 5-year savings will be ($600 - $30) x 3.79 - $1.2K = $1K.

See the risk analysis worksheets in Section B.14 of Appendix B.

RECOMMENDATION:

Use personal information to validate the caller's identity. Send notification of the address change to the old address.

3.2.1.2.5 AUDITING/TRAINING

BACKGROUND AND INTRODUCTION:

The Auditing Unit for each functional area of operations at the Twoville field office reports to the general supervisor for that functional area. All auditing is for the purpose of quality control.

FINDING 3.2.1.2.5-1

Auditors in the Twoville field office report to the heads of the units they audit.

RELATED CONTROL STANDARD 5137(C)(3):

Similar concepts of split duties must be used in critical controls and financial functions. For example, special controls involving more than one person must be established over blank an voided checks.

DISCUSSION:

There is a conflict of interest when the supervisor of a particular function also has control over the auditing of that function. An overly ambitious supervisor could attempt to make the performance of his people look better than it really was by influencing the activity of the auditors. In particular, the supervisors can prevent the auditors form increasing the level of surveillance of particular employees.

It is our opinion that audit activities should be totally independent of the function being audited.

RISK ANALYSIS:

Because there is no opportunity here for direct material gain, we select the AFE to be .006, the low end of the range for fraud and abuse.

If a supervisor is able to control the auditing activity and gain access to the auditors' detailed work schedules, he might be able to warn claims processors that a particular day's work will be

reviewed so that they an be at their best performance level.

For the remainder of the time the processors would naturally tend to put speed ahead of quality, knowing that they will not be audited and that incentive pay is available for exceeding the production standards.

The result would be an excessive error rate by all affected processors on non-audit days. It would be reasonable to assume that the excessive errors would require half an hour per day per processor to correct. This means that 1/2 / 8 = 1/16 of each processor's working time would be wasted. There are approximately 180 processors (not counting the Telephones Unit) at the Twoville and Threeville field offices. Their average pay is about $5.50 per hour. Using the overhead rate of 25%, their total yearly cost to SOES is 180 processors x 1.25 overhead x $5.50/hr x 8 hrs/day x 5 days/wk x 52 wks/yr = $2.5M.

The ALE is .006 x $2.5M = $15K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The safeguard is to reorganize the Twoville and Threeville field offices so that the auditors report directly to the respective office managers. This safeguard should have a negligible one-time cost and should reduce the ALE by 95%.

The savings will then be ($15K - $1.5K) = $14K per year.

See the risk analysis worksheets in Section B.15 of Appendix B.

RECOMMENDATION:

The auditors should report directly to the field office manager.

3.2.1.2.6 TSI SUPPORT

BACKGROUND AND INTRODUCTION

The TSI support function at Twoville is very similar to that at Fourville. An onsite systems analyst trainee assists the field office staff with software problems and local hardware problems.

We found no problems with the practices and procedures of the TSI support personnel at Twoville.

3.2.1.2.7 PERSONNEL

BACKGROUND AND INTRODUCTION

The Personnel Unit (1 person currently assigned) handles all personnel matters for the Fourville and Twoville field offices.

3.2.1.3 THREEVILLE FIELD OFFICE

BACKGROUND AND INTRODUCTION:

The Threeville field office is currently responsible for the direct data entry of claims as well as the correspondence processing associated with these claims. Eventually, Threeville will handle all aspects of the processing of these claims.

FINDING 3.2.1.3-1:

The main entrance of the Threeville field office is not monitored during the early morning and late afternoon.

RELATED CONTROL STANDARD 5137(N)(2):

Control must also be maintained in other Unemployment Insurance Bureau work areas over the presence of visitors, and the presence of employees after normal working hours.

DISCUSSION:

This problem is similar to that of Finding 3.2.1.1-2. Because the Threeville field office has other physical access control problems, however all are treated together in Finding 2.7-4. The risk analysis and cost-benefit analysis are omitted here as they would be repetitive.

RISK ANALYSIS:

N/A

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION:

Ensure that the reception area is staffed at all times when the main entrance door is unlocked. Alternatively, install a bell or

other signaling device which will sound when the door is opened from the outside.

FINDING 3.2.1.3-2:

Documents describing restricted access software are not given special protection at the Threeville field office.

RELATED CONTROL STANDARD 5137(N)(1):

All the Unemployment Insurance Bureau assets and related operations must be secured against unauthorized access; this includes sensitive data in transit within the organization.

DISCUSSION:

This problem is identical to that of Finding 3.2.1.2-4. The risk analysis and cost-benefit analysis of that finding take both Twoville and Threeville into account and are not repeated here.

RISK ANALYSIS:

N/A

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

RECOMMENDATION

Access to restricted software should be controlled through passwords or user security profiles, not through the secrecy of operating procedures. In the present situation, the restricted documents should be stored in locked desks or cabinets.

3.2.1.3.1 DATA ENTRY

BACKGROUND AND INTRODUCTION

The direct data entry function is carried out by six units currently operating under a single general supervisor. A correspondence unit and a training and auditing unit also report to the same supervisor.

We found no problems with the practices and procedures of this unit.

3.2.1.3.2 CORRESPONDENCE

BACKGROUND AND INTRODUCTION

There is a single Correspondence Unit at Threeville which reports to the same general supervisor as the six data entry units and the Training and Auditing Unit.

Problems related to correspondence processing are similar to those at Twoville. See Section 3.2.1.2.2 for details.

3.2.1.3.3 AUDITING AND TRAINING

BACKGROUND AND INTRODUCTION:

This unit performs quality control audits of the data entry and correspondence functions and trains newly hired personnel in these areas as well as in the auditing area.

The unit reports to the same general supervisor as the six data entry units and the Correspondence Unit.

FINDING 3.2.1.2.3-1:

The Correspondence Unit auditor reports directly to the head of the Correspondence Unit at the Threeville filed office. The data entry auditors report to the General Supervisor of the data entry units.

RELATED CONTROL STANDARD 5137(C)(4):

Similar concepts of split duties must be used in critical control and financial functions. For example, special controls involving more than one person must be established over blank and voided checks.

DISCUSSION:

Supervision of both an operation and the auditing of that operation represents a conflict of interest. This finding is similar to finding 3.2.1.2.5-1. Supervisors of operational units should not be allowed to challenge the activities of the auditors as they can at the Threeville field office.

RISK ANALYSIS:

The analysis is done under Finding 3.2.1.2.5-1 and is not repeated here.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

See Finding 3.2.1.2.5-1

RECOMMENDATION:

All auditors should report directly to the field office manager.

FINDING 3.2.1.3.3-2:

The Training/Auditing supervisor must relinquish most auditing responsibilities to the General Supervisor when training classes are in session.

RELATED CONTROL STANDARD 5137(C)(4):

Similar concepts of split duties must be used in critical control and financial functions. For example, special controls involving more than one person must be established over blank and voided checks.

DISCUSSION:

The training and auditing workloads are too heavy for a single person when training classes are in session. The General Supervisor must assume the audit role at such times. This results in a potentially non-uniform approach to auditing and a more serious conflict of interest than is normally the case.

The finding is closely related to Finding 3.2.1.3.3-1. Consequently, the risk analysis is not repeated here.

RECOMMENDATION:

Assign the audit responsibility to a single person reporting directly to the field office manager.

3.2.1.3.4 TURNKEY SYSTEMS INC. (TSI) SUPPORT

BACKGROUND AND INTRODUCTION:

In addition to software and local hardware support, TSI provides and staffs a data center at Threeville which is co-located with the SOES field office.

The data center operates two independent IBM 4341 mainframes which

accumulate transactions from Twoville, Threeville and Fourville as well as the other field offices and transmit them to the TSI Main Data Center in Capitaltown. Each system can serve as backup for the other. If the dedicated lines to Capitaltown go down, connection can be re-established through a dial backup capability. When the mainframe in Capitaltown in down, the Threeville Data Center can continue to accept and store transactions until it is brought online again.

The overall systems design provides for such excellent backup that loss of the data entry capability (except due to power failure or virtual destruction of the Threeville Data Center) is extremely unlikely.

FINDING 3.2.1.3.4-1:

The backup A/C unit for the Threeville Data Center is not periodically tested.

RELATED CONTROL STANDARD 5137(Q)(4):

In the event of a disaster or disruption, the computer facility and the backup facility must have the capability to function normally with minimal delay or lost processing time.

DISCUSSION:

The backup A/C unit is on the roof. Although there was an instance when the main A/C unit failed and the backup unit did not respond, the backup unit is still not subjected to periodic testing or rotated into regular operational use.

RISK ANALYSIS:

Failure of the backup A/C unit could force a halt to operation of the Threeville Data Center. Experience has shown that with exhaust fans, the center cent operated for about three hours after an A/C failure. That should be sufficient time for an A/C serviceman to fix a minor problem. Major problems requiring special parts may take longer. We estimate that such problems can be expected once per year and will require a full day to repair. Most of that time would be spent awaiting the arrival of parts. The AFE is thus 1. The loss to SOES would be 5 hours of processing which would then have to be done in overtime. The additional cost would be half the regular pay of about 97 DDE processors and 16 correspondence processors. The average hourly

rates are about $5.85 for DDE and $6 for Correspondence.

The loss would be 5 hrs x 1.25 overhead x [(97 data entry processors x $5.85/hr + (16 corr. processors x $6.00/hr)] = $4.1K.

The ALE is thus $4.1K x 1 = $4.1K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

Regular testing of the backup A/C unit will eliminate the problem entirely and will cost a negligible amount.

The ALE will be reduced to $0. The savings will be $4.1K per year.

See the risk analysis worksheets in Section B.16 of Appendix B.

RECOMMENDATION:

Test the backup A/C unit on a regular basis.

FINDING 3.2.1.3.4-2

Visitor access records are not kept at the Threeville Data Center.

RELATED CONTROL STANDARD 5137(N)(9):

Access to all EDP operation areas is to be controlled and a record maintained of access by other than EDP operations personnel. (Permanent onsite maintenance personnel and designated pickup and delivery personnel are considered "operations personnel".

DISCUSSION:

Without access records it is impossible to make a connection between security violations discovered after the fact and the presence of visitors who may have been responsible for the violations.

RISK ANALYSIS:

Although no access records are kept, visitors to the Threeville Data Center are few and generally have official business there. It is very unlikely that such a visitor would attempt to cause any harm. We assign an AFE of .001 taken from the low end of the scale for terrorism and other destructive acts.

Because we are examining a problem in which the presence or absence of visitor records is a determining factor, the damage done by our hypothetical visitor would have to be such as not to become evident until well after his departure, but this is not a difficult matter.

The loss to SOES would be the loss in processing time resulting from any damage done to the Threeville Data Center. As much as two weeks might be lost if a difficult to replace item of equipment wee involved.

The cost to make up these two weeks in overtime would be 1.5 overtime x (130 staff) x (1.25 overhead) x (2 wks) x (40 hrs/wk) x $6/hr = $117K.

The ALE is then $117K x .001 = $120.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

Visitor access records should be kept. The cost would be negligible for such a small data center. The savings would result from using the access records to trace the identity of a malefactor and obtain restitution. Part of the restitution would be the cost of the overtime operations made necessary by the destructive act.

The records would reduce the ALE by only 50% because it is not at all certain that a problem can be connected with a particular visitor even if his identity is known.

The new ALE is $60. The savings will be ($120 - $60) - $0 = $60 per year.

See the risk analysis worksheets in Section B.17 of Appendix B.

RECOMMENDATION:

Keep records of visitor access to the Threeville Data Center.

FINDING 3.2.1.3.4-3:

There are no underfloor water detectors at the Threeville Data Center.

RELATED CONTROL STANDARD 5137(O):

Valuable equipment or sensitive data must be separated from hazards if other safeguards are not feasible or cost effective (e.g., relocate kitchen out from under computer room or tape library away from heating plant boilers.)

DISCUSSION:

The risk analysis for this finding is included under Finding 2.2-1 and is not repeated here. This finding is especially significant in light of the potential for flooding at the Threeville field office location identified in Finding 2.2-1.

RISK ANALYSIS:

N/A

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION:

Install underfloor water detectors at the Threeville Data Center.

3.2.1.3.5 PERSONNEL

BACKGROUND AND INTRODUCTION:

Personnel services at Threeville are provided by a representative who reports to the Sixville area office of SOES.

We found no problems in the practices and procedures of this unit.

3.2.2 UNEMPLOYMENT INSURANCE BUREAU MANAGEMENT SERVICES

BACKGROUND AND INTRODUCTION:

This group oversees the generation and distribution of about 30 periodically produced reports required by DOL/UIS and SOES. All are derived from computer output.

The group is also responsible for the development, maintenance and enhancement of the detailed claims processing procedures used in headquarters and the three field offices.

Management Services is additionally developing and marketing two electronic claims submission systems. One will allow employers to

submit wage record data on magnetic tape. The other will allow them to submit the data online via telephone.

Unemployment Insurance Bureau Management Services also acts as an interface between the SOES Unemployment Insurance Bureau and TSI for directing the CUIS development, enhancement and maintenance functions. The group coordinates and approves change requests within SOES, transmits them to TSI and monitors and evaluates the resulting programming effort.

The group is lastly responsible for the maintenance of various computer files including employer and claimant correspondence and the full range of edit and audit tests which are applied to all incoming Unemployment Insurance Bureau claims.

We found no problems with the practices and procedures of this office.

3.2.3 LIAISON AND EMPLOYER AUDIT AND REVIEW

BACKGROUND AND INTRODUCTION:

This group acts as an interface between the Unemployment Insurance Bureau and all other organizational elements including DOL/UIS and other SOES departments such as Accounting which provide services to the Unemployment Insurance Bureau.

The group also conducts fair hearings on appeals by claimants of the handling of Unemployment Insurance Bureau claims.

In the area of employer audit and review, the group performs initial reviews and periodic audits. It also operates a Program Integrity Unit to collect information on instances of fraud and abuse and pass it on to the appropriate authorities.

3.2.3.1 EMPLOYER AUDIT AND REVIEW

BACKGROUND AND INTRODUCTION:

This Section consists of the Initial Employer Review Unit, Employer Audit Unit, and the Program Integrity Unit.

3.2.3.1.1 INITIAL EMPLOYER REVIEW UNIT

BACKGROUND AND INTRODUCTION:

This unit collects profile, staffing and salary data on new employers and enters it into the computer system through CUIS. A profile analysis program then compares this data to statistical averages of data initially supplied by employers later caught in a variety of fraudulent schemes. The program assigns a risk code which then controls the triggering of future reviews of the employer.

We found no problems with the practices or procedures of this unit.

3.2.3.1.2 EMPLOYER AUDIT UNIT

BACKGROUND AND INTRODUCTION:

This unit carries out reviews of wage record reporting and tax payments which fail the CUIS audit criteria and of claims involving employers who are on review because of suspected irregularities in their tax payment procedures.

When a discrepancy is found, the employer involved may be referred to a reviewer, placed on chargeable claims review, or referred to Program Integrity. Alternatively, recoupment action may be initiated or consultation may be sought with the offending claimant.

FINDING 3.2.3.1.2-1:

It would be possible for a reviewer to form a conspiracy for purposes of fraud with an employer for who he's responsible.

RELATED CONTROL STANDARD 5137(C)(1):

Organizations must employ effective measures, consistent with their operational environment, to limit the potential for unassisted fraud. For example, a computer console operator should not be allowed to write programs and introduce them into the system, or to introduce any programs not authorized by someone responsible for internal control, such as the tape librarian.

Further examples of duties that should not be assigned the same employee at the same time are scheduling, operating, programming, storage, and the library functions; nor should employees be allowed to perform unassigned duties that might increase their range of activities.

DISCUSSION:

In most situations, a SOES employer reviewer could not conspire with an outsider to process claims in a fraudulent manner because he could not guarantee that the fraudulent claims would be assigned to him for review.

However, for some industries, there is only one reviewer assigned. When a claim deals with a particular industry, the one qualified reviewer is assured of processing it.

RISK ANALYSIS:

The potential for fraud here is estimated at $100K per year. This figure is obtained by estimating the size and number of claims that would be fraudulently processed in the course of a year. Small claims would not be worth the effort. An excessive number of claims would be dangerous. We have estimated 1000 claims per year at $100 each.

Because of the need for a conspiracy in this case, an AFE of .006 has been chosen, the low end of the range for fraud and abuse.

The ALE is $100K x .006 = $600.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

Ensure that more than one reviewer is available for each industry. This will create an effective separation of duties in that no one person will then have full control over one particular aspect of employer review.

The cost of adding reviewer staff should be negligible as all are paid on the basis of work done, not as full-time employees of SOES.

This safeguard should reduce the AFE by 75%. Even with additional reviewers, some claims will find their way to a conspirator. Those that do not will most likely be denied if they are unjustified.

Because of this possibility of denial, fraudulent claims will have to be more subtly prepared and less frequently submitted. The new ALE would be 200 claims by $100 claim x (.006 x .25) = $30.

The savings will be ($600 - $30) = $570.

See the risk analysis worksheets in Section B.18 of Appendix B.

RECOMMENDATION:

Provide more than one possible processor for each aspect of claims processing.

3.2.3.1.3 PROGRAM INTEGRITY

BACKGROUND AND INTRODUCTION:

Program Integrity collects information from all available sources concerning fraud and abuse in the Unemployment Insurance program. About 440 cases per year are handled. Of these, 380 prove to be false alarms. The remaining 60 are reported to the State Department of Justice (SDOJ). Of these, 10 are eventually cleared and SDOJ directs SOES to pursue recoupment in the other 50.

We found no problems with the practices and procedures of this unit.

3.2.3.2 LIAISON

BACKGROUND AND INTRODUCTION:

This group acts as an interface between the Unemployment Insurance Bureau and other organizational elements having dealings with or providing services to the Unemployment Insurance Bureau. This includes other SOES departments, DOL/UIS and other external groups.

The group also processes appeals of Unemployment Insurance Bureau claims dispositions through the Fair Hearings Section.

3.2.3.2.1 LIAISON

BACKGROUND AND INTRODUCTION:

This section provides the interface with other elements described in Section 3.2.3.2.

We found no problems with the practices or procedures of this unit.

3.2.3.2.2 FAIR HEARINGS

BACKGROUND AND INTRODUCTION:

This section processes appeals of claim dispositions by Unemployment Insurance Bureau claimants and payees.

We found no problems with the practices or procedures of this unit.

3.2.4 EMPLOYER TAX RECORDS

BACKGROUND AND INTRODUCTION:

This office serves all of SOES's programs. It maintains an integrated Master Employer File which contains information about employers. The office is responsible for deleting employers as well as updating information on employers already in the file.

FINDING 3.2.4-1:

There is no effective control to ensure that employers who cease doing business or leave the area are purged from the Master Employer File.

RELATED CONTROL STANDARD 5137(B)(3):

The Unemployment Insurance Bureau must establish a retention schedule monitoring procedure for all UI data.

DISCUSSION:

Employers who remain on the master file although they are no longer active in the area could be impersonated by individuals attempting to defraud the Unemployment Insurance Bureau benefit payment fund.

Currently, employers are removed from the file as a result of returned mail and information received from employer review field contacts.

RISK ANALYSIS:

Lists of employers who have ceased doing business in the State and are potentially still on the Master Employer File can be obtained in a variety of ways requiring only a little ingenuity and effort. For example, most telephone books have lists of employers by trade in the Yellow Pages. A comparison of the current and previous editions would provide the desired information.

An inquiry to SOES by a concerned claimant might then confirm that an employer is still on file.

Continuing in this fashion, it would be possible to acquire all the information necessary to use a departed employer for the purpose of filing phoney claims.

As before, a reasonable tradeoff on the total number and size of claims filed in this manner would be about 1,000 claims per year at $100 per claim or $100K per year. The middle of the frequency scale for fraud and abuse yields an AFE of .03.

The ALE is then $100K x .03 = $3K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The safeguard is to devise a set of procedures to ensure the currency of the Master Employer File. This might include periodic verifications that employers are still doing business in The State and could be done on the basis of the potential for fraud presented by the dollar volume of Unemployment Insurance Bureau claims being filed by the terminated employees of particular employers. We estimate that this safeguard would cost two staff-weeks of development effort at the grade 32 level and one hour per day of CRT operations at the OE level to process the verification transactions.

The cost would be 1.25 overhead x 80 hrs x $10.44/hr = $1K for development (one-time) and 1.25 overhead x 5 days/wk x52 weeks x 1 hr/day x $7.45/hr = $2.4K per year for verification processing.

The ALE will be reduced by 90% to $300.

The 5-year savings will be 3.79 x $3K - 3.79 x $300 - 3.79 x $2.4K - $1K = $160.

See the risk analysis worksheets in Section B.19 of Appendix B.

RECOMMENDATION:

Investigate ways to improve the accuracy and currency of the Master Employer File.

FINDING 3.2.4-2:

Although signatures are required on documents requesting Master

Employer File updates, the signatures are not verified.

RELATED CONTROL STANDARD 5137(K)(5):

Establish appropriate controls over all sensitive data entering or leaving the facility, employing a system that will preclude erroneous or unauthorized transfer of data, regardless of media or format. These controls must include the maintenance of a record for the logging of shipping and receipts, and periodic reconciliation of these records.

DISCUSSION:

Without verification, impostors could cause changes to be made to the Master employer File which result in funds being diverted from the intended recipients. Signature verification does not require professional handwriting analysis. It is done as a matter of course by store clerks who receive checks from customers.

RISK ANALYSIS:

This finding goes hand-in-hand with Finding 3.2.4-1 above. Once a swindler determines the name of an employer he can exploit, he must either change the employer's address so that the can control correspondence with SOES. The approach he takes will depend on whether or not he has access to legitimate Unemployment Insurance Bureau claimants as well as other considerations.

We feel that the two findings are so closely related that separate risk analyses would unreasonably inflate the loss potential associated with inadequacies in Master Employer File management. Consequently, the quantification of this finding is included in finding 3.2.4-1.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION

Verify signatures on Master Employer File update requests.

3.3 TURNKEY SYSTEMS INC. SOFTWARE SUPPORT (HEADQUARTERS)

BACKGROUND AND INTRODUCTION:

This TSI group operates under Unemployment Insurance Bureau contract to provide all software support services for the Comprehensive Unemployment Insurance System (CUIS). CUIS consists of a number of online and batch subsystems. There are about 1,680 modules in CUIS, 70% of which are in assembly language and 30% in COBOL. Altogether, there are about 4.2 million lines of source code in CUIS.

The TSI Software Support Group consists of three development/maintenance teams in capitalville, three teams in Sevenville, an Industrial Engineer, a Customer Support Unit which provides onsite technical assistance in the field offices and the Threeville Data Center staff.

FINDING 3.3-1:

There is no effective separation between CUIS development, testing and maintenance activities and production operations.

RELATED CONTROL STANDARD 5137(C)(1):

Organizations must employ effective measures, consistent with their operational environment, to limit the potential for unassisted fraud. For example, a computer console operator should not be allowed to write programs and introduce them into the system, or to introduce programs not authorized by someone responsible for internal control, such as a tape librarian. Further examples of duties that should not be assigned the same employee at the same time are scheduling, operating, programming, storage, and the library functions; nor should employees be allowed to perform unassigned duties that might increase the range of their activities.

RELATED CONTROL STANDARD 5137(C)(3):

Test data must not contain actual information which can be linked to specific individuals. If old files containing personal data are used, names, addresses, and other identifiers must be modified to make the personal data meaningless, unless a parallel production run is being performed using live data.

DISCUSSION:

Separation of duties is an important control which can be used to hinder fraud and abuse by employees. It requires that no single employee be given *all* the authorities that would be necessary to transfer assets outside the organization or to make

changes in operational procedures or the controls over operational procedures.

If a single employee had the ability to write a check on Bureau funds, for example, he could convert those funds to his own use.

If a single employee had the authority to modify the code of the CUIS system *and* to enter transactions which would result in the payment of Unemployment Insurance Bureau benefits, he could easily arrange for his own fraudulent claims to by pass edits and audits and be paid.

If, however, such critical duties and authorities are split among two or more employees, collusion will be required in order to defraud the organization successfully. If is always more difficult to effect a criminal partnership than to operate alone. One can never be certain that a co-worker will not immediately report an attempt to solicit his assistance in a criminal venture.

Even if a partnership can be successfully formed, all parties must be constantly concerned about the possibility of being double-crossed or betrayed.

The issue of this finding is that separation of duties is not effectively used to isolate software development, maintenance and testing activities from production operations.

It is generally accepted good practice to assure that all production software is approved by two or more development/maintenance analysts prior to being placed into production and that one in production those analysts be restricted from further modifying the software.

The development/maintenance personnel should at no time have access to the production data files.

Modifications should be triggered only by an assessment from the use or production operations personnel that the software is not functioning properly or that changes are required.

When such an assessment is made, copies of the affected production software modules should be passed by production operations to development/maintenance personnel. The same formal approval cycle is then used again in returning these modules to production after they have been modified and tested.

In the case of SOES Unemployment Insurance Bureau Operations, the TSI personnel who develop, maintain and test CUIS also have full access to the operational Unemployment Insurance Bureau data files. It is also possible for a single TSI analyst to make code modifications to CUIS without review by a second party. Although the analyst could not personally inert the modifications into the production software library directly, he could obtain all the necessary approvals based on his word and on the success of testing.

It would thus be possible for a software analyst to make surreptitious changes to CUIS which would leave CUIS with its full intended functionality but which would also allow the analyst to subvert the system under circumstances known only to him. We do not mean to imply that any personnel currently working with CUIS would abuse their position in this way. We do mean to state that the controls necessary to prevent such an abuse of trust are not present.

As an example of how an unscrupulous software analyst might proceed, consider the following scenario. The analyst, intent on defrauding the system; uses his knowledge of CUIS to determine what kinds of changes would help him and where in CUIS those changes would have to be applied. After forming a list of such potential changes, he waits until he is assigned a small maintenance task (one not likely to be reviewed by other analysts) involving the module or modules he wishes to change. He then makes the required changes as well as his own secret changes.

The secret changes will be such that they will have no effect on CUIS operation unless invoked by a predetermined pattern of claims data, a special codeword entered at a CRT terminal or some other circumstance unlikely to arise by chance.

Consequently, testing will not reveal the presence of the secret changes. Because the changes are not desk-checked by a second analyst, they will not be discovered and will be installed in the production CUIS system.

The analyst can then use his ability to enter transactions into the production CUIS system to put his secret changes to work.

RISK ANALYSIS:

Because of the lack of separation of access to CUIS production software and Unemployment Insurance Bureau data files, the Unemployment Insurance Bureau benefit fund is vulnerable to fraud

and abuse by software support personnel.

The loss potential in this case is th full $500K reported by the FBI to be the average loss resulting from a computer fraud. We use the higher figure here because of the unique potential for abuse resulting from the accessibility of both CUIS programs and Unemployment Insurance Bureau data files.

The AFE taken from the middle of the range of frequencies for fraud and abuse is .03.

The ALE is $500K x .03 = $15K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The suggested safeguard is to apply the principle of separation of duties. TSI software support personnel should have full access to the development version of the CUIS software but not to the production version and not to the production Unemployment Insurance Bureau data files.

Data file access should be limited to SOES personnel and/or TSI personnel who do not have access to the CUIS software.

Achieving the goal of separation of duties in the software area will require an analysis of the present situation, a plan for realignment of activities and possibly some additional staff time.

We estimate the cost to be 3 staff-months of analysis and planning and one staff member quarter-time to coordinate software support with data file access.

We have used a salary of $30K and 100% overhead for the analysis and planning task and a grade 30 salary with 25% overhead for the coordination tasks.

The safeguard thus has a one-time cost of 1/4 yr x 2.0 overhead x $30K/yr = $15 and a continuing cost of 1/4 yr x 1.25 overhead x $19,947/yr = $6.2K.

The ALE should be reduced by 90% to $1.5K.

The 5-year savings will be 3.79 x ($15k - $1.5K) - 3.79 x $6.2K - $15K = $13K.

See the risk analysis worksheets in Section B.20 of Appendix B.

RECOMMENDATION:

Provide for the effective separation of the development maintenance and testing of application systems and the production operation of those systems.

FINDING 3.3-2:

It is possible for a single person to carry out all steps necessary to insert a software modification into the production CUIS system without independent review.

RELATED CONTROL STANDARD 5137(C)(1):

Organizations must employ effective measures, consistent with their operational environment, to limit the potential for unassisted fraud. For example, a computer console operator should not be allowed to write programs not authorized by someone responsible for internal control, such as the tape librarian. Further examples of duties that should not be assigned to the same employee at the same time are scheduling, operating, programming, storage, and library functions; nor should employees be allowed to perform unassigned duties that might increase the range of their activities.

DISCUSSION:

This finding actually represents one aspect of Finding 3.3-1 above. It is listed separately because it can be addressed separately. However, for risk analysis purposes, this finding will be treated as part of Finding 3.3-1.

RECOMMENDATION:

Ensure that all changes, additions and deletions to production CUIS software are reviewed by at least one analyst not involved in their preparation.

FINDING 3.3-3:

Journalization of CUIS transactions is incomplete.

RELATED CONTROL STANDARD 5137(H)(1):

Every attempt to update the data file must be logged to both the location and the individual doing the updating. The log or the

journal must show what information was changed and the date. Such journals must be periodically reviewed:

DISCUSSION:

To provide for full data integrity it is necessary that every data item be traceable form its time of original entry, through all intermediate changes up to whatever time an inquiry is made. This means that every transaction resulting in a change to the data item must be recorded along with the ID of the person entering it.

This transaction journal file must be maintained for as long as it is intended that the integrity of the related data be accountable.

We were informed that the 10 most recent modifications to a SOES Unemployment Insurance Bureau claim are journalized indefinitely and that less than 1% of claims would undergo so much change that information would be lost.

It is our opinion that journalization should be complete.

RISK ANALYSIS:

The fact that only the 10 most recent changes are saved could be used to hide fraudulent changes. The procedure would be to make the fraudulent change and then make 10 legitimate changes.

Such an approach could not be used too frequently because a pattern of claims with excessive changes would result and might be detected and investigated.

This technique of suppressing journalization is one of a number of techniques which might support fraudulent activity by software support personnel (Finding 3.3-1) or by claims processors (Finding 3.2.1.1.2-1).

A separate risk analysis of this finding would be repetitive and has thus not been done.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION:

Provide for complete journalization of CUIS transactions.

FINDING 3.3-4:

Restricted CUIS subsystems are protected by secret clerk numbers coded into the software.

RELATED CONTROL STANDARD 5137(J)(12):

Passwords must not be displayed on the video display terminals or hardcopy devices. Ensure that computer operators, acting without authority, are not able to display user programs or circumvent security mechanisms.

DISCUSSION:

The use of secret clerk numbers would not constitute a problem all by itself. The coding of the secret numbers directly into application software modules does constitute a problem, however. It results in the need to protect the source code of those modules much more stringently than would otherwise be required.

It is normally necessary to protect source code from long term access by unauthorized persons in order to prevent those persons from becoming sufficiently familiar with the structure of the software to plan an attack against it.

However, secret clerk numbers can be picked out of a source code listing very rapidly by an experienced analyst. Source code containing such secret data must then be protected from very short term access by unauthorized parties. This of course means that listings cannot be left unattended on desks for short periods of time.

Whether or not it contains secret codewords, the source version of production software should not be readable by all system users. The privilege of reading as well as writing production source should be restricted to those with a need to do so.

RISK ANALYSIS:

This finding concerns a weakness which could be exploited by anyone with a knowledge of CUIS and read access to CUIS source. A separate risk analysis of this finding would be repetitive because of its close relationship to Finding 3.3-1.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

RECOMMENDATION:

Use the ACF2 Security Software to protect restricted CUIS modules where possible.

FINDING 3.3-5:

The CUIS Software Support Group does not enforce periodic changes of passwords and permits the selection of passwords with mnemonic value.

RELATED CONTROL STANDARD 5137(J)(11):

Passwords must be modified at periodic unannounced intervals, when an individual changes positions, and when a security breach is suspected.

DISCUSSION:

Passwords with mnemonic value are much more easily guessed than random passwords. Passwords should be selected through the use of random number generators. The resulting character strings can be selected in such a way that they are pronounceable but should consist of nonsense syllables only.

RISK ANALYSIS:

This is another vulnerability which can be exploited by persons familiar with CUIS software and data who have access to Unemployment Insurance Bureau CRTs. The risk analysis of this finding is contained in that of Finding 3.3-1 and is not repeated here.

SUGGESTEED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION:

Enforce periodic changes of passwords. Do not allow the use of passwords with mnemonic value (other than perhaps pronounceability).

FINDING 3.3-6:

CUIS is not supported to the fullest extent possible by ACF2.

RELATED CONTROL STANDARD 5137(J)(7):

The supervisory mode of the on-line system must be limited to terminals restricted for supervisory use, and not be available to all terminals.

DISCUSSION:

To provide access control, secret clerk Ids have been coded into some of the CUIS modules, a much less desirable alternative than having system software responsible for the management and storing of passwords. (see Finding 3.3-4.)

ACF2 should be used to control access to the various capabilities of CUIS by claims processors.

Because this finding is closely related to Finding 3.3-1, a separate risk analysis would be repetitive. The finding is stated as it is here because it provides a different viewpoint for the same problem.

RECOMMENDATION:

Use AFC2 to serve all the security needs of online CUIS subsystems.

3.3.1 FE TEAM

BACKGROUND AND INTRODUCTION:

This is the first of the three Capitaltown-based CUIS development/maintenance teams. It is responsible for the front end (FE) or online claims processing software.

We found no problems which were unique to the FE Team. Problems common to all teams are discussed in Section 3.3 above.

3.3.2 B TEAM

BACKGROUND AND INTRODUCTION:

This is the second of the Capitaltown-based CUIS development/maintenance teams. It is responsible for batch (B) claims processing software.

We found no problems unique to the B team. Problems common to all

teams are discussed in Section 3.3 above.

3.3.3 SYSTEM SUPPORT

BACKGROUND AND INTRODUCTION:

This is the third of the Capitaltown-based CUIS development/maintenance teams. Because it is responsible for the software which supports the Master Employer File, this team serves all SOES activities, not just the Unemployment Insurance Bureau. The team also maintains the Unemployment Insurance Bureau disbursement profiles, the complex tables of payments which will be authorized for each category of benefit.

3.4 TURNKEY SYSTEMS INC. MAIN DATA CENTER

BACKGROUND AND INTRODUCTION:

The TSI Main Data Center in Capitaltown serves government and commercial customers across the State. About 20% of the center's business is the SOES Unemployment Insurance Bureau. Other customers include banks, retailers and other government agencies.

The center operates two IBM 3033 mainframes, either of which can handle the complete online CUIS load.

The data center staff covers all functional areas involved in the operation of a modern large-scale computer department.

3.4.1 MAIN DATA CENTER SECURITY

BACKGROUND AND INTRODUCTION:

This is a staff position reporting to the Operations Manager. The position covers all aspects of physical security for the data center.

FINDING 3.4.1-1:

C02 is in use in the data center as a fire suppressant. It is potentially harmful to personnel.

RELATED CONTROL STANDARD 5137(J)(1)(c):

Avoid the use of carbon dioxide area extinguishing systems since they present a significant safety hazard.

DISCUSSION:

The CO2 for this system is stored in metal tanks in the utility room containing the three motor-generators. It is set to discharge under the raised floor of the main computer room. Seven times the total amount of C02 available would be required to protect the entire computer room. By design, there is only enough to protect the underfloor area. There would be no protection , other than hand-held extinguishers against a major above-floor fire.

RISK ANALYSIS:

The loss to SOES might occur through a lawsuit brought by the estate of a person who is trapped in the data center during the release of C02 and suffocates.

The AFE for such a loss is the product of two frequency estimates: the estimate for fires which set off the C02 extinguishing system and the estimate for a person being trapped and succumbing given that a fire breaks out and the C02 is released.

From national statistics in Appendix A, the AFE for a serious fire is .01.

Several factors have a bearing on the likelihood of a person being trapped. The C02 is released under the floor and because its density is greater than that of air, will tend to stay there. The regular data center staff has been warned about the danger.

On the other hand, the C02 releasing system is pressurized and will thus tend to force the gas to rise above the floor. Also, visitors are not routinely warned of the danger.

We feel that the likelihood of a person being trapped and suffocating under these circumstances very small. An AFE of .001 has been assigned.

The loss, if it occurs, would be on the order of $1M in damage awards and $20K in legal fees. The ALE is thus $1M x .01 x .001 = $10.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The safeguard is to convert the fire suppression system from C02 to halon 1301. Halon can be used at a level of concentration that

will extinguish fires but will not injure personnel. The cost of this is estimated at $20K.

The ALE will be reduced to $0.

The safeguard is not cost-effective, but some change away from C02 is advised.

See the risk analysis worksheets in Section B.21 of Appendix B.

RECOMMENDATION:

Provide full flood halon protection for the entire data center.

FINDING 3.4.1-2:

There is no visitor sign-in policy at the data center.

RELATED CONTROL STANDARD 5137(N)(9):

Access to all EDP operations areas is to be controlled and a record maintained of access by other than the EDP operations personnel. (Permanent onsite maintenance personnel and designated pickup and delivery personnel are considered "operations personnel).

DISCUSSION:

Records of visitor access to the data center should be recorded at all times. Whereas regular employees are all likely to enter the data center during normal working hours, only an access control log can provide a complete record of visitors.

Criteria for escorting visitors should also be established.

RISK ANALYSIS:

This finding is related to the problem of controlling physical access to the data center. If an unauthorized person were able to enter he could steal equipment or data and/or do damage to the facility which would interrupt computer operations for as much as four weeks.

A number of other findings deal with vulnerabilities which could lead to unauthorized access to the data center. All such findings are assessed collectively here.

The loss to SOES if this were to occur would be greatest if it led to a disaster causing a four week shutdown of operations. The cost of such a shutdown would be the cost of overtime necessary to catch up after operations were restored. This cost would be 1.5 overtime x 260 processors x $6/hr x 40 hrs/wk x 4 wks x 1.25 overhead = $470K.

The AFE for such an event is taken from the national statistics on destructive acts. It is unlikely that an intruder could simply walk into the data center without advance planning and preparation. The existing access control vulnerabilities require skill and daring to exploit and have led us to choose an AFE at the low end of the range. This AFE is 1.

The ALE is then $470 x 1 = $40K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The safeguard needed here is a tightening of data center access controls.

The blue badge stripe authorizing data center access should be replaced with a more difficult to duplicate token placed entirely under the lamination. Attempts to remove this token from a badge should result in its mutilation.

Records of al visitor access to the data center should be maintained.

Requests to sign out tapes from the media library should be validated.

The cost of these safeguards should not exceed 3-staff months to define and plan and one staff-day per week to implement. Using a salary level of $30K per year for planning and $18K per year for implementation, and an overhead factor of 100% (typical for contractors), the one-time cost will be 1/4 yr x (2.0 overhead) x $30K/yr = $15K. The recurring cost will be 1/5 yr x (2.0 overhead) x $18K/yr = $7.2K per year.

The ALE reduction will be about 75%. The reduced ALE will be 1/4 x $470K = $120K.

The 5-year savings will be ($470K - $120K) x 3.79 - $7.2K x 3.79 - $15K = $1.3M.

See the risk analysis worksheets in Section B.22 of Appendix B.

RECOMMENDATION:

Implement a visitor sign-in policy for the data center. Validate tape sign-out requests. Modify the badge token authorizing data center access.

FINDING 3.4.1-3:

The blue ID badge stripe which authorizes data center access can be easily forged.

RELATED CONTROL STANDARD 5137(N)(1):

All Unemployment Insurance Bureau assets and related operations must be secured against unauthorized access; this includes sensitive data in transit within the contractor's organization. Custody and responsibility ceases at the point where the data is turned over to the U.S. Post Office or other reliable carrier.

DISCUSSION:

The blue stripe which authorizes access to the data center consists of a piece of blue tape attached to the badge form horizontally above the employee picture and sealed by the lamination.

This credential could be easily faked by placing the tape stripe over the lamination and then placing a second laminating layer over the first.

RISK ANALYSIS:

See related Finding 3.4.1-2.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION:

In place of the blue stripe, use a difficult to duplicate marking such as an engraved design and attach it to the ID badge under the lamination. It then becomes impossible to add or remove this credential once a badge has been completely assembled, and the

counterfeiting process is much more difficult than before.

FINDING 3.4.1-4:

Fire protection by C02 is provided only for the underfloor areas of the data center.

RELATED CONTROL STANDARD 5137(J)(1)(B):

Fire extinguishing equipment will vary in accordance with the physical characteristics of the facility and is subject to local regulations. After ensuring that appropriate arrangements have been made for fire fighting assistance, management should use either water or halon systems if area extinguishing systems are determined to be necessary.

DISCUSSION:

This problem is covered under Finding 3.4.1-1. It is stated here in order to bring attention to a separate aspect of the problem.

RECOMMENDATION:

Install a full-flood halon system in the data center.

FINDING 3.4.1-5:

The key to the storage area containing blank Unemployment Insurance Bureau benefit checks is kept on a hook near the computer console operator. The access list for the key contains 30 names.

RELATED CONTROL STANDARD 5137(N)(1):

All Unemployment Insurance Bureau assets and related operations must be secured against unauthorized access; this includes sensitive data in transit within the organization.

DISCUSSION:

Access to the key should be restricted to as few people as possible. If one person and an alternate on each shift (regular plus weekend) were assigned responsibility for the key, most situations should be covered. Adding a few higher level supervisors to the list should take care of virtually all circumstances.

The list should not contain more than about 15 names. It should also be satisfactory to store the key in the locked wall box in the output processing area. This area is very close to the locked supply cage anyway, and there is little advantage to storing the key on a hook near the console operator where it is not nearly as well protected.

RISK ANALYSIS:

This finding relates to physical access control in the data center. The risk analysis is presented under Finding 3.4.1-2 and is not repeated here.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION

Pare down the access list for the key to the Unemployment Insurance Bureau blank check storage area. Maintain all copies of the key in protected or continuously monitored storage locations.

FINDING 3.4.1-6:

There are no alarms and only hand-held fire extinguishers in the supply area adjacent to the main computer room.

RELATED CONTROL STANDARD 5137(I)(2):

In the computer room, install fire detection equipment that includes alarms. The alarm systems should be capable of indicating where the activated alarm is located.

DISCUSSION:

This problem is related to Findings 3.4.1-4 and 3.4.1-1. Because all three findings are related, the risk analysis and cost-benefit analysis are done only once (under Finding 3.4.1-1).

The finding is stated separately here to call attention to a different aspect of the problem.

The supply area is the area most vulnerable to the starting of a fire and at the same time the area least protected.

RECOMMENDATION:

Upgrade the fire detection and suppression equipment in the data center supply storage area.

FINDING 3.4.1-7:

There is no smoke exhaust capability in the data center.

RELATED CONTROL STANDARD 5137(P)(1):

Equip all computer operations areas with a smoke exhaust capability to minimize the potential hazard to personnel, equipment, and storage media. Equip air conditioning ductwork systems with dampers to prevent the spread of fire, smoke or chemical agents.

DISCUSSION:

Although portable fans are on hand for cooling down overhead equipment and could be used for smoke exhaust purposes, no thought has been given to the problem and no plan for exhausting smoke has been prepared.

RISK ANALYSIS:

A smoke exhaust system can only be used after the danger of spreading fire has been eliminated. The system would possibly have an effect on the chances for survival of any persons trapped in the computer center during a fire. There would be no effect on material damages due to the fire itself.

We wee no losses to SOES due to the absence of a smoke exhaust system.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

In spite of the $0 ALE, requirements call for a smoke exhaust capability in all computer operations areas.

We recommend that the effectiveness of the portable fans in exhausting smoke be reviewed and if necessary, alternative methods chosen.

In all probability, it will be sufficient to draft an emergency procedure specifying how the portable fans should be placed to maximize their smoke exhaust capabilities.

The cost of the effectiveness study and procedure preparation should not exceed one staff-month at a salary level of $20K with 100% overhead. the cost would be 1/12 yr x 2.0 overhead x $20K/yr = $3.7K. Although the safeguard is not directly cost effective, it is required by the State.

See the risk analysis worksheets in section B.23 of Appendix B.

RECOMMENDATION:

Formalize the use of portable fans for exhausting smoke.

3.4.2 SYSTEMS SOFTWARE

BACKGROUND AND INTRODUCTION:

This group provides support for the operating system, all IBM program products and other proprietary software packages.

FINDING 3.4.2-1:

There is no provision for the real-time on-line reporting of incorrect password usage attempts to a security officer.

RELATED CONTROL STANDARD 5137(J)(5):

For on-line systems, limit the number of sign-on attempts and, when the limit is exceeded, generate an alert to the individual responsible for on-line security.

DISCUSSION:

Without on-line reporting of incorrect password entry attempts, it is difficult if not impossible to catch computer system intruders. An audit trail of all sign-ons, successful or not, would aid in identifying persons who perform unauthorized activities on the computer system.

RISK ANALYSIS:

This problem is similar in effect to Finding 3.2.1.2.3-1 in that it allows attempts at unauthorized access to CUIS to go undetected. This weakness has been accounted for in the AFE selection made under that finding. The risk analysis is not repeated here.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION:

Provide for the online reporting of incorrect password entry attempts.

3.4.3 ONLINE APPLICATIONS

BACKGROUND AND INTRODUCTION:

This group currently provides no support to SOES Unemployment Insurance Bureau operations. The group does maintain the ODCS security subsystem which is not but could be used to protect that portion of CUIS originally designed to operated under ODCS (as opposed to CICS). ODCS is the On-line Data Communications System, a predecessor to CICS designed and developed by Turnkey Systems, Inc. (TSI).

3.4.4 TECH SUPPORT/RTI DIVISION

BACKGROUND AND INTRODUCTION:

This division provides technical assistance to operations and System Engineers (SEs) in the field. It also operates a run-time improvement (RTI) program by reviewing PROCS for optimum coding and assists new data center accounts with their processing.

About 15% of this division's activities are in support of the SOES Unemployment Insurance Bureau.

The ACF2 Security Software is this division's responsibility.

FINDING 3.4.4-1:

The data center has no policy requiring periodic changes to passwords. Users are allowed to specify their own passwords.

RELATED CONTROL STANDARD 5137(J)(11):

Passwords must be modified at periodic unannounced intervals, when an individual changes positions, and when a security breach is suspected.

DISCUSSION:

The TSI data center supports a number of corporate customers who process sensitive information. It would thus be wise to require these customers to observe a certain amount of procedural discipline for their own protection.

A major part of this discipline would be to require periodic changes of passwords and random selection of passwords.

This finding is related to Finding 3.3-1 and the risk analysis and cost-benefit analysis are not repeated here. The purpose of this finding is to point out the separate responsibilities of the CUIS Software Support Group and the TSI Main Data Center to provide for the security of their operations.

RECOMMENDATION:

The data center should require the use of randomly generated passwords which are changed at least once a year.

3.4.5 DATA MANAGEMENT DIVISION

BACKGROUND AND INTRODUCTION:

This division is responsible for tape library operations and the Mini Computer Group.

3.4.5.1 TAPE LIBRARY

BACKGROUND AND INTRODUCTION:

The tape library is responsible for all aspects of tape operations and management. The Tape Library Management System (TLMS) provides support in this area.

FINDING 3.4.5.1-1:

No authorization checks are made when tapes are signed out from the tape library.

RELATED CONTROL STANDARD 5137(N)(1):

All unemployment Insurance Bureau assets and related operations must be secured against unauthorized access; this includes sensitive data in transit within the contractor's organization.

DISSCUSSION:

When an individual attempts to sign out a tape from the tape library, the only check made on his authority to do so is to ensure that he has an ID badge with the blue stripe indicating data center access. This of course does not identify him in any way as the owner of the tape. Also, as discussed in Finding 3.4.1-3, the blue stripe is simple to forge. Thus anyone with a SOES picture badge could remove a tape from the library without too much effort.

RISK ANALYSIS:

Loss to SOES because of this, problems could occur in a number of ways. A stolen tape could cause a processing delay of up to a day while the backup was being fetched and updated. A stolen tape could be modified for purposes of fraud on a compatible computer system and then replaced in the library. A stolen tape could be used by an individual for activities in violation of the State Privacy act which would leave SOES vulnerable to lawsuits for not providing proper protection fro such data.

The latter scenarios described above lead to the largest loss potentials. We set the loss potential at $100K.

The AFE of .006 is taken from the low end of the frequency scale for fraud and abuse because of the effort required to exploit this vulnerability.

The ALE is $100K x .006 = $600.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The safeguard is to validate sign-out requests. This can be done with negligible additional cost by verifying that the tape owner is either making or has authorized the sign-out request.

The ALE will be reduced to $0.

The savings will be $600 per year.

See the risk analysis worksheets in Section B.24 of Appendix B.

RECOMMENDATION:

Release tapes only to their owners or to persons authorized in

writing by the owners.

FINDINGS 3.4.5.1-2:

Non-production tapes are scratched automatically when the retention data is reached.

RELATED CONTROL STANDARD 5137(C)(6):

Routines that modify the status volume serial number of a file must be controlled. This means the authority to scratch, or rename a rile must be limited and controlled.

DISCUSSION:

Owners of tapes should be notified of approaching scratch dates so that they can be assured of an opportunity to request an extension. It is too easy to lose track of retention dates especially when dealing with a large number of tapes.

The tape Library Management System (TLMS) could automatically prepare for each owner a list of tapes owned and the corresponding retention dates. Such a list could be prepared periodically (e.g. monthly). The owners could then indicate any retention date changes and return the list to the library for action.

NOTE: **This is not a problem with CUIS** *production* **tapes.**

RISK ANALYSIS:

The loss to SOES in this case would be the cost of regenerating the contents of a tape scratched accidentally. The problem could result not only from the rigid observance of retention dates but also from mismounts and other mistakes. It is unlikely that a production data file would be scratched in this manner because most such files are on disk and production tape files have indefinite retention. Accidents are possible, however.

The average tape is 9-track, 2400 feet long, and contains 1,600 bytes per inch. If full, the tape would contain 1,600 bytes/in x 12 1n/ft x 1,200 ft = 23M bytes, allowing half the length of the tape for inter-record gaps containing no data.

In the worst case, no backup will exist and the entire contents of the tape will have to be key-entered. An experienced data entry

clerk can key 90 words per minute. At 5 characters (or bytes) per work on the average, this is the equivalent of 5 bytes/work x 90 words/min x 60 min/hr = 27K bytes/hr.

Approximately 23M/27K = 850 hours would be required for the data entry at a cost of not more than $6/hr x 850 hrs x 1.25 overhead = $6.4K.

No statistics were available on the number of tapes scratched accidentally at the Main Data Center. National statistics predict a range of 12 to 24 accidental scratches per year.

Using the lower end of the range, we select an AFE of 12. We also recognize that backup tapes might exist, but not more than half the time because private (i.e. non-production) tapes are most susceptible and these are not likely to have backups in more than 50% of the cases.

The ALE is $6.4K x .5 x 12= $38K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

the safeguard is to consult the owner prior to scratching tapes. The TLMS system is capable of producing inventory lists by owner with retention dates. Each tape owner's list should be sent to him for review once per moth to indicate any needed retention date changes.

The cost would be one man-day per month maximum on the part of tape library personnel. At a salary of $18K with 100% overhead, the cost would be (1/2) yr x $18K/yr x 2.0 overhead = $3K.

The ALE would be reduced by 75%. The remaining 25% of inappropriate scratches would be done accidentally.

The reduced ALE is .25 x $30K = $9.5K.

The savings will be ($38K - $9.5K) - $1.7K = $27K per year.

See the risk analysis worksheets in Section B.25 of Appendix B.

RECOMMENDATION:

Consult tape owners prior to scratching tapes whose retention dates have passed.

FINDING 3.4.5.1-3:

Tapes are not degassed after scratching and prior to reuse.

RELATED CONTROL STANDARD 5137(M):

SECURE DISPOSAL - Dispose of all retired, discarded or unneeded sensitive data in a way that makes it impossible for unauthorized personnel to obtain it.

DISCUSSION:

Because tapes are not degaussed prior to reuse and because they are not reserved for use by individual data center customers, it is possible for one customer to scavenge another customer's old data by requesting a scratch tape and reading it before writing it.

Scavenging of tapes within a single customer organization is also a potentially serious problem. In this situation a resourceful but unprincipled SOES employee might simply browse through old tapes until he located something useful or interesting such as the source listing of a CUIS module containing an access code or an old wage record tape.

RISK ANALYSIS:

The loss to SOES caused by the failure to degauss scratched tapes would seem to be a secondary effect. The person who detects something of interest on a scratched tape would then have to make use of what he finds. He might find employer numbers and addresses and use them on phoney claims. He might find CUIS source code containing an access password and attempt to gain unauthorized access to that part of CUIS.

The effects of this vulnerability are accounted for in the other findings of this report. The risk analyses are not repeated here.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

N/A

RECOMMENDATION:

Degauss all scratch tapes prior to reissue.

3.4.5.2 MINI COMPUTER GROUP

BACKGROUND AND INTRODUCTION:

This group manages the operation of several mini computers. Only one of these, the Downline Loading System (DLS), is operated in support of the Unemployment Insurance Bureau. The DLS is used to send system software modifications directly to the Threeville Data Center from Capitaltown so that on-site SE support requirements at Threeville can be held to a minimum. testing of the Threeville system can also be done from Capitaltown via the DLS.

We found no problems with the practices or procedures of this unit.

3.4.6 ONLINE/RJE DIVISION

BACKGROUND AND INTRODUCTION:

The Online/RJE Division is responsible for teleprocessing hardware, and network operations. With respect to the Unemployment Insurance Bureau, the division initializes CUIS each morning and assures that all data files are open and operable. It also receives calls from the field. Performance-related problems are dealt with either directly or through outside support. Other types of problems are referred to the appropriate group.

3.4.7 OUTPUT CONTROL DIVISION:

The division is responsible for data and forms control, the operation of conventional and laser printers and the distribution of output.

We found no problems with the practices and procedures of this division.

3.5 ACCOUNTING SERVICES

BACKGROUND AND INTRODUCTION:

This department is responsible for all accounting activities at SOES including bank account management, fund reconciliation, the handling of returned and recouped funds and the disbursement of claim payments.

3.5.1 PROGRAMS ACCOUNTING

BACKGROUND AND INTRODUCTION:

This office handles the accounting for the Unemployment Insurance Bureau program as well as other SOES programs.

FINDINGS 3.5.1-1:

Secure areas used by the Programs Accounting Department have walls which do not extend to the true ceiling.

RELATED CONTROL STANDARD 5137(N)(19):

Provide for the secure storage of all media containing sensitive data when it is not is use.

DISCUSSION:

The Accounting Department uses one locked storeroom to hold blank check stock, a second locked room for the occasional overnight storage of printed and signed checks and a third room (the Cash Receiving area) for the storage of checks returned by the Postal Service as undeliverable.

All three of these room have walls which extend only as for as the dropped ceiling tiles. It is a trivial matter to lift out ceiling tiles and climb over the false wall into the storage area.

RISK ANALYSIS:

The easiest way to take advantage of this vulnerability would be to climb over the wall into the Cash receiving area (or break down the upper half of the Dutch door which is secured only by a single sliding bar latch) and steal some checks that were returned by the Postal Service due to incorrect addresses. There is a large number of these checks on file and some are for amounts in the $10K range.

These large checks are usually tax refunds sent to employers who move all or part of their operations out of state and take most of the affected employees with them. If done properly, the theft will not be detected until the checks clear the bank or possibly later.

The loss to SOES might be as much as $100K.

The frequency estimate, taken from the low end of the range for theft is 1.

The ALE is $100K x 1 = $100K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The safeguard is to extend the walls of all storage areas to the true ceiling and to alarm all doors and windows leading to these areas.

The cost will be no more than $2K per room. For 3 rooms the total would be $6K.

The ALE will be reduced by 50% to $50K. the reduction will not be greater because the returned checks are still susceptible to theft by employees of the Cash Receiving Unit. In Finding 3.5.1-2, a second safeguard will be proposed to eliminate the remaining ALE.

The 5-year savings will be ($100K - $50K) x 3.79 - $6 = $184K.

See risk analysis worksheets in Section B.26 of Appendix B.

RECOMMENDATOIN:

Extend the walls of all secure storage areas to meet the true ceiling.

FINDING 3.5.1-2:

Benefit checks returned to SOES are not batched and present an easy target for abuse.

RELATED CONTROL STANDARD 5137(N)(1):

All Unemployment Insurance Bureau assets and related operations must be secured against unauthorized access; this includes sensitive data in transit within the organization. Custody and responsibility ceases at the point where the data is turned over to the U.S. Post Office or other reliable carrier.

DISCUSSION:

Benefit checks returned as undeliverable by the Postal service are easily recognized by mailroom personnel because of the distinctive envelopes in which they are sent out.

They are sent unopened and unbatched to the Cash Receiving area. It would be a simple matter for a mailroom clerk or a cash

receiving clerk to remove some of the checks and attempt to cash them or sell them to a fence.

RISK ANALYSIS:

This finding is similar to the previous finding in that the targeted asset is the same. In the present situation, the threat agent will have no obstacle (such as false walls) to overcome because as a Cash Receiving employee he has access to the returned checks on a regular basis.

On the other hand, such an employee would be more vulnerable to detection than an outsider who could disappear without his identity ever becoming known.

We do not feel that this finding increases the ALE due to misappropriation of returned checks in Finding 3.5.1-1.

The ALE is thus $50K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The main issue of this finding is the lack of controls which would lead to the immediate detection of a missing check.

Although the finding does not lead to an increased ALE, it does suggest a means of eliminating the $50K ALE remaining from Finding 3.5.1-1. If returned checks are destroyed immediately and then reissued if and when the recipient's correct address comes to light, the entire problem of returned checks will be eliminated.

The cost of this safeguard will be a half hour per day for batching the returned checks in the mailroom and zero additional time for Cash Receiving to place the checks in a secure container for disposal instead of in a file cabinet.

Using the salary of a grade QC mailroom clerk, this cost will be 1/2 hr/day x 5 days/wk x 52 wks/yr x $6.76/hr x 1.25 overhead = $1.1K.

The ALE will be reduced to $0 from $50K.

The savings will be ($50K - $1.1K) = $49 per year.

See the risk analysis worksheets in Section B.27 of Appendix B.

RECOMMENDATION:

Batch returned checks in the mailroom prior to sending them to Cash Receiving. Then destroy the checks after generating the necessary accounting records.

3.6 LEGAL AFFAIRS

BACKGROUND AND INTRODUCTION:

Legal Affairs provides contracting assistance to the Unemployment Insurance Bureau, monitors federal legislation for Unemployment Insurance Bureau-related issues and serves as a source of information for opposing legal counsel in court cases.

We found no problems with the practices or procedures of this unit.

3.7 CONSUMER AFFAIRS

BACKGROUND AND INTRODUCTION:

Consumer Affairs processes VIP queries relating to the Unemployment Insurance Bureau and monitors claimant litigation in order to protect SOES's interests.

We found no problems with the practices or procedures of this unit.

3.8 GENERAL AUDIT

BACKGROUND AND INTRODUCTION:

General Audit is responsible for all Headquarters financial audit activities and reports to the Assistant Director for Management.

FINDING 3.8-1:

When an audit is to be conducted, advance notice is given to the affected department.

RELATED CONTROL STANDARD 5137(N)(10):

Supervisors have certain responsibilities for the security and integrity of data in their work area. They must be instructed to monitor the activities of the visitors to the work area (including company employees from other work areas), and to ensure that

functions of the unit are performed only by employees formally assigned to the unit. Supervisors should have procedures for handling questionable activities.

DISCUSSION:

Normally only one day advance notice is given. This would be more than sufficient time for an embezzler to remove any incriminating records or complete any cover-up activities.

It is our position that records to be examined in an audit should be secured by the auditors with absolutely no advance notice whatsoever.

RISK ANALYSIS:

The loss to SOES in this situation would be due to a failure to detect and recoup misappropriated funds.

The loss potential is estimated at $100K.

The AFE of .006 is selected from the lower end of the range for fraud and abuse. The AFE is modified by a factor of .5 to allow for the possibility that the perpetrator will not learn of the impending audit and fail to cover his tracks in time.

The ALE is $100K x .006 x.5 = $300.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The safeguard is to initiate all audits on a surprise basis and collect all records to be reviewed immediately after announcing the audit to the affected department.

The cost of this safeguard is $0.

The ALE will be reduced by 90% to $30. In the other 10% of cases, the perpetrator will not be vulnerable to an audit at the critical time when records are collected.

The savings will be $270 per year.

See the risk analysis worksheets in Section B.28 of Appendix B.

RECOMMENDATION:

As a matter of policy, give no notice of impending audit activity to the affected departments.

3.9 PLANS AND RESEARCH

BACKGROUND AND INTRODUCTION:

This department develops broad goals and objectives for all SOES activities. It monitors each area of activity and provides feedback when necessary.

We found no problems with the practices and procedures of this department.

3.10 PERSONNEL ADMINISTRATION

BACKGROUND AND INTRODUCTION:

This department is responsible for hiring, salary administration, employee relations, labor union negotiations and all other aspects of personnel administration.

3.10.1 COMPENSATION AND BENEFITS

BACKGROUND AND INTRODUCTION:

This office is responsible for ensuring a competitive salary structure at SOES. It also administers the employee benefits program and conducts union wage negotiations. Position classification, performance appraisals and coordination of personnel activities in the eastern half of the state are other areas of involvement.

We found no problems with the practices and procedures of this unit.

3.10.2 EMPLOYEE/LABOR RELATIONS

BACKGROUND AND INTRODUCTION:

This office assists in union negotiations, formulates labor relations policy, ensures SOES compliance with the union contract and performs related duties as directed.

We found no problem with the practices and procedures of this office.

3.10.3 EMPLOYEE SELECTION/DEVELOPMENT

BACKGROUND AND INTRODUCTION:

This office determines the needs of SOES in the area of employee development and sets up programs to satisfy those needs. It also plans and directs employment activities and runs the EEO program.

We found no problems with the practices and procedures of this office.

3.11 GENERAL SERVICES

BACKGROUND AND INTRODUCTION:

General Services is responsible for all matters concerning physical facilities, incoming and outgoing mail, the procurement of goods and services, word processing, reproduction, the headquarters telephone switchboard and forms management.

3.11.1 FACILITIES

BACKGROUND AND INTRODUCTION:

Facilities is responsible for all matters concerning the SOES physical plant including leases, guard service, fire protection, etc.

We found no problems with the practices and procedures of this unit.

3.11.2 MAIL AND DISTRIBUTION

BACKGROUND AND INTRODUCTION:

Mail and distribution receives, sorts and distributes incoming mail from the Postal Service and other carriers. it also processes outgoing mail.

FINING 3.11.2-1:

The storeroom used by the Mail and Distribution Department has walls which do not extend to the true ceiling as well as unalarmed exterior windows.

RELATED CONTROL STANDARD 5137(N)(9):

Provide for the secure storage of all media containing sensitive data when it is not in sue.

DISCUSSION:

This is another instance of the problem discussed in Finding 3.5.1-1. In this case, the storage room has walls which do not extend to the true ceiling and unalarmed windows. The room is used to store 5 to 10 Unemployment Insurance Bureau benefit checks overnight once or twice per week.

RISK ANALYSIS:

The checks stored in this room could be stolen. An insider would wait until one or more large checks were to be stored overnight. The average value of a check is about $200. A large check might be worth $5K to $10K. We set the loss potential at $10K for the worst case.

The AFE of 1 is taken from the low end of the range for theft.

The ALE is $10K x 1 = $10K.

SUGGESTED SAFEGUARDS AND COST-BENEFIT ANALYSIS:

The safeguard is to alarm the door and windows in this room and to extend the walls to the true ceiling. The cost will not exceed $2K.

The ALE will be reduced to $0.

The 5-year savings will be 3.79 x ($10K - $0) - $2K = $3.6K.

See the risk analysis worksheets in Section B.29 of Appendix B.

RECOMMENDATION:

Extend the walls of all secure storage areas to meet the true ceiling.

3.11.3 MATERIEL SERVICES

BACKGROUND AND INTRODUCTION:

Material Services is responsible for all purchasing, warehousing and records storage within SOES.

We found no problems with the practices and procedures of this unit.