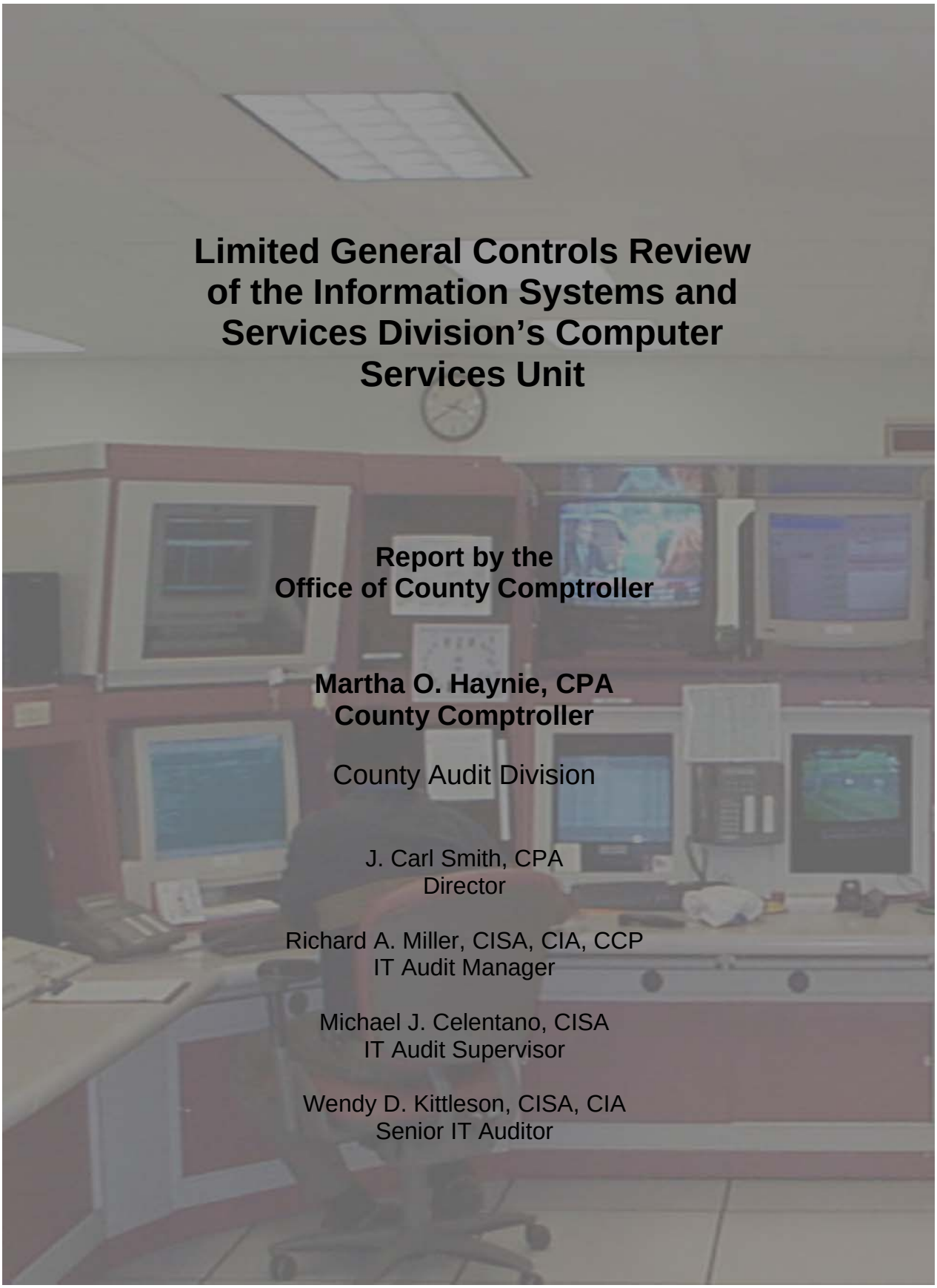

Limited General Controls Review of the Information Systems and Services Division's Computer Services Unit

Report by the
Office of County Comptroller

Martha O. Haynie, CPA
County Comptroller

County Audit Division

J. Carl Smith, CPA
Director

Richard A. Miller, CISA, CIA, CCP
IT Audit Manager

Michael J. Celentano, CISA
IT Audit Supervisor

Wendy D. Kittleson, CISA, CIA
Senior IT Auditor

Report No. 351
July 2004

TABLE OF CONTENTS

July 19, 2004

Richard T. Crotty, County Chairman
And
Board of County Commissioners

We have conducted a limited general controls review of the Orange County Information Systems and Services Division's (ISS) Computing Services Unit (CSU) as of February 28, 2003. The audit did not include a review of contingency planning and data security functions, nor applications processed on the various equipment operated by computer operations. The audit was conducted in accordance with generally accepted government auditing standards and the Information Systems Audit and Control Association's IS Auditing Standards, and included such tests as we considered necessary in the circumstances.

Responses to our Recommendations for Improvement were received from the Chief Information Officer, Information Systems and Services Division and are incorporated herein.

We appreciate the cooperation of the personnel of the CSU during the course of the audit.

Martha O. Haynie, CPA
County Comptroller

c: Ajit Lalchandani, County Administrator
Warren Gelch, Director, Administrative Services Department
Rafael Mena, Chief Information Officer, Information Systems and Services Division
Jim Harvey, Unit Supervisor, Computer Services Unit

EXECUTIVE SUMMARY

Executive Summary

We have conducted a limited general controls audit of the Orange County Information Systems and Services (ISS) Division's Computing Services Unit (CSU). We reviewed the system of internal control in effect as of February 28, 2003. Our audit was conducted in accordance with generally accepted government auditing standards and the Information Systems Audit and Control Association's IS Auditing Standards, and included such tests as we considered necessary in the circumstances.

ISS provides support services to operating departments and elected officials in areas such as customer computer applications and software, data processing, data communication, telephone, and radio. CSU provides a twenty-four hour, seven days a week, secured, controlled environment for Orange County's computer systems. They provide disaster recovery support for all of the mission-critical applications housed within CSU including mainframe, Unix, and server applications.

Our objective was to provide reasonable assurance that controls exist to ensure the security of assets and resources through appropriate policies and procedures. To determine if this objective was met, we interviewed management and staff, reviewed existing policy, procedure and standards manuals, and observed work being performed.

This report presents specific control weaknesses that we identified during the course of the audit. We have communicated to management other matters that are not significant enough to warrant inclusion in this report.

Based on our review and evaluation, we conclude that internal controls were adequate except for the issuance of temporary access badges, the notification process for removing terminated employee access, the establishment of a comprehensive IT security program and control weaknesses identified in the application change control process.

Temporary access badges are issued to visitors at the Regional Computing Center (RCC). Controls over this process do not include a review that would identify missing badges in a timely manner so corrective action could be taken. Our inventory identified two badges that have been missing since November 2002.

An IT Security program has not been developed and communicated to the user community that would provide a continuous assessment of security risks to assure continued effectiveness of policies and procedures.

Procedures that require an employee's supervisor to notify Security Administration of terminated or transferred employees and contracted personnel are infrequently followed. In addition, procedures have not been developed to periodically require user departments to re-certify their employees' access is appropriate.

Production Control has been processing changes that could have a significant impact on applications without the appropriate level of supervisory approval. Further, the role of the appropriately designated user representative has not been addressed.

Management concurred or partially concurred with all of the recommendations made in this report and corrective action is either completed, planned, or underway.

ACTION PLAN

LIMITED GENERAL CONTROLS REVIEW OF THE INFORMATION SYSTEMS AND SERVICES DIVISION'S COMPUTER SERVICES UNIT
ACTION PLAN

NO.	RECOMMENDATIONS	MANAGEMENT RESPONSE			IMPLEMENTATION STATUS	
		CONCUR	PARTIALLY CONCUR	DO NOT CONCUR	UNDERWAY	PLANNED
1.	We recommend procedures be developed and implemented that assure the timely identification of missing temporary badges. All badges should be returned by the end of each day and any outstanding badges should be accounted for before the responsible employee leaves for the day. The status of those badges not returned the night before should be followed up on and reconciled promptly the next day. All discrepancies should be escalated to management for prompt corrective action.	✓			✓	
2.	We recommend:					
A)	Access to the RCC, the computer room, and network center should be restricted to the RCC staff required to support daily operations and RCC building access badge profiles should be adjusted accordingly based on each individual's assigned work schedule.	✓			Completed	
B)	All work outside of regularly scheduled work hours be logged.	✓			✓	
C)	The access log should be periodically reviewed for questionable trends, and escalated to management for corrective action, when identified.	✓			✓	
3.	We recommend procedures be developed and implemented that establish and document the annual verification of individuals authorized to enter the RCC, the computer room and network center. The results of this annual review should be used to update the existing "Physical Access to Computer Room" and "Employees Authorized to Access Computer Room" policies and guidelines. In addition, RCC building access badge profiles should be adjusted accordingly.	✓			✓	

LIMITED GENERAL CONTROLS REVIEW OF THE INFORMATION SYSTEMS AND SERVICES DIVISION'S COMPUTER SERVICES UNIT
ACTION PLAN

NO.	RECOMMENDATIONS	MANAGEMENT RESPONSE			IMPLEMENTATION STATUS	
		CONCUR	PARTIALLY CONCUR	DO NOT CONCUR	UNDERWAY	PLANNED
4.	We recommend Security Administration develops and implements policies and procedures:					
A)	Requiring user management to notify Security Administration immediately upon employee termination or transfer;	✓			✓	
B)	To routinely advise user management of the need to promptly notify Security Administration of terminated or transferred employees and contracted personnel;	✓			✓	
C)	Periodically requesting user management review and re-certify user access, including contracted personnel, and confirm, based on access lists provided by Security Administration, that each user's access is appropriate based on their assigned job duties; and	✓			✓	
D)	To ensure that all contracted personnel are contractually required to adhere to County and ISS policies and procedures (including but not limited to internet usage, e-mail, security and confidentiality.)	✓			✓	
5.	We recommend ISS management develops and implements a comprehensive security program that includes the continuous assessment of security risks and links the results of those assessments to existing policies and procedures to assure their continued effectiveness. Further, ISS management should review the security program annually to assure it remains in compliance with the County's goals and objectives.	✓				✓

LIMITED GENERAL CONTROLS REVIEW OF THE INFORMATION SYSTEMS AND SERVICES DIVISION'S COMPUTER SERVICES UNIT
ACTION PLAN

NO.	RECOMMENDATIONS	MANAGEMENT RESPONSE			IMPLEMENTATION STATUS	
		CONCUR	PARTIALLY CONCUR	DO NOT CONCUR	UNDERWAY	PLANNED
6.	We recommend a completed change request form be submitted to the Production Control Supervisor with appropriately designated user representative and Systems Development Unit Supervisor approvals prior to the implementation of high-risk software changes to production applications.	✓				✓
7.	We recommend a completed change request form be submitted to the Production Control Supervisor with appropriately designated user representative and project leader approvals prior to routine software changes being implemented to production applications.	✓				✓
8.	We recommend emergency software change procedures be followed for changes that are in fact the result of emergency conditions. In addition, Production Control personnel should ensure that appropriate approvals are obtained for all emergency changes and that problem reports have been included in change documentation. Further, procedures should be developed and implemented for changes requiring priority implementation schedules and they should conform to regular change control procedures.	✓				✓
9.	We recommend ISS management periodically reviews and updates policies and procedures to ensure they are current and conform to management's established directives.	✓				✓
10.	We recommend Security Administration distributes security violation reports to appropriate User Management for follow-up and resolution of identified violations.	✓				✓

LIMITED GENERAL CONTROLS REVIEW OF THE INFORMATION SYSTEMS AND SERVICES DIVISION'S COMPUTER SERVICES UNIT
ACTION PLAN

NO.	RECOMMENDATIONS	MANAGEMENT RESPONSE			IMPLEMENTATION STATUS	
		CONCUR	PARTIALLY CONCUR	DO NOT CONCUR	UNDERWAY	PLANNED
11.	We recommend:					
A)	Access to CA Scheduler be restricted to Production Control and Computer Operations personnel as required to perform their job responsibilities**.**	✓			Completed	
B)	Manager privileges to CA Scheduler be limited to two people within Production Control; the person assigned the responsibility for adding users and their backup.	✓			Completed	
12.	We recommend each CA Scheduler user be assigned a unique User ID and password.	✓			Completed	
13.	We recommend ISS personnel:					
A)	Assures all maintenance agreements are on-hand for reference;	✓			Completed	
B)	Obtains and reviews the agreement with EMC Corporation to assure authorization requirements, confidentiality and proficiency of technical staff are addressed;	✓			Completed	
C)	Ensures that all future vendor agreements require vendor adherence to County and ISS policies and procedures (including but not limited to internet usage, e-mail, security, confidentiality, etc.); and	✓				✓
D)	Ensures that all future vendor agreements include provisions for security responsibilities and procedures.	✓				✓
14.	We recommend CSU personnel establishes procedures to ensure that preventative maintenance is performed according to contractual arrangements and defined schedules.	✓				✓
15.	We recommend CSU personnel:					
A)	Obtains a current listing of the equipment covered under the IBM maintenance contract and reconcile it with the current inventory;	✓			Completed	

LIMITED GENERAL CONTROLS REVIEW OF THE INFORMATION SYSTEMS AND SERVICES DIVISION'S COMPUTER SERVICES UNIT
ACTION PLAN

NO.	RECOMMENDATIONS	MANAGEMENT RESPONSE			IMPLEMENTATION STATUS	
		CONCUR	PARTIALLY CONCUR	DO NOT CONCUR	UNDERWAY	PLANNED
15. B)	Updates or establishes procedures for the timely notification of additions and deletions to maintenance contracts; and	✓			Completed	
C)	Updates or establishes procedures to review and reconcile vendor-supplied quarterly reports.	✓			Completed	
16.	We recommend:					
A)	Service level agreements, that establish system availability, response time, and job turnaround targets, should be established, agreed to and documented for all major user groups.		✓			✓
B)	A periodic review of agreements in effect should be performed to assure they are maintained in a current fashion.		✓			✓
C)	The service level agreement with Corrections should be updated, re-negotiated, and formalized.		✓			✓
17.	We recommend management measures the achievement of objectives for major ISS projects. Specifically, project milestones and deliverables that include cost and completion timeframes should be measured, evaluated, and corrective action implemented where necessary.	✓				✓
18.	We recommend cost comparisons be prepared and documented for significant projects. In addition, appropriate management approval should be obtained and documented for projects undertaken by ISS before committing funds and resources.	✓				✓

LIMITED GENERAL CONTROLS REVIEW OF THE INFORMATION SYSTEMS AND SERVICES DIVISION'S COMPUTER SERVICES UNIT
ACTION PLAN

NO.	RECOMMENDATIONS	MANAGEMENT RESPONSE			IMPLEMENTATION STATUS	
		CONCUR	PARTIALLY CONCUR	DO NOT CONCUR	UNDERWAY	PLANNED
19.	We recommend procedures be developed and implemented that require documented approval before the purchase requisition data is forwarded to the Purchasing and Contracts Division. If purchasing authority is delegated by the Division Head, it should be documented as to who has the authority, the limits of authority and the duration of the authority. The person preparing the requisition should use this information to verify purchase requests have been properly authorized. In addition, supporting documentation should be retained that provides evidence of the substance of the transaction as well as its approval.	✓			Completed	
20.	We recommend a procedure be established and implemented that assures the accuracy of sources of funds used in purchase requisitions electronically submitted to the Purchasing and Contracts Department.	✓			Completed	
21.	We recommend ISS management:					
A)	Performs and documents a formal risk assessment, for all functions within ISS and implements and documents a level of security commensurate with the risks identified;	✓				✓
B)	Develops and implements procedures to update risk assessments as changes occur; and	✓				✓
C)	Develops and implements procedures that require an annual review of risk assessments to assure a continued level of adequate security.	✓				✓
22.	We recommend security guidelines and procedures be routinely communicated to the user community and that periodic security awareness training be conducted for current and newly hired employees.	✓				✓

LIMITED GENERAL CONTROLS REVIEW OF THE INFORMATION SYSTEMS AND SERVICES DIVISION'S COMPUTER SERVICES UNIT
ACTION PLAN

NO.	RECOMMENDATIONS	MANAGEMENT RESPONSE			IMPLEMENTATION STATUS	
		CONCUR	PARTIALLY CONCUR	DO NOT CONCUR	UNDERWAY	PLANNED
23.	We recommend ISS management:					
A)	Reviews and updates security policies and procedures to reflect currently approved operating procedures; and	✓				✓
B)	Reviews and approves the section addressing security and integrity at least annually.	✓				✓

INTRODUCTION

Background

Information Systems and Services (ISS) provides support services to all operating departments and elected officials in areas such as customer computer applications and software, data processing, data communication, telephone, and radio.

Computing Services Unit (CSU) provides a twenty-four hour, seven days a week, secure, controlled environment for Orange County's computer systems that involves monitoring building security and environmental control systems at the RCC. Operational support is provided for applications that are maintained on the mainframe and ensures scheduled jobs are processed completely. They provide Disaster Recovery support for all of the mission-critical applications housed within the CSU, including both mainframe and server applications.

CSU also provides after-hours technical support for the help desk and is in charge of printing reports and distributing them to the requesting division.

The Production Control section within CSU manages the job scheduling software and assures processes are run in the proper sequence and at the appropriate time. In addition, Production Control provides support for changes to production applications and is the final review before these changes are moved into a production environment.

Scope, Objectives, and Methodology

The audit scope was limited to an examination of general controls relative to the Information Systems and Services Division's CSU located at the RCC as of February 28, 2003. The limited audit neither included a review of contingency planning and data security functions nor a review of applications processed on the various equipment operated by computer operations.

The objectives of the audit were to determine on a limited basis through interviews and discussions that:

- Objectives for the area under review are met and performance is monitored;

- Policies and procedures are documented and adequate;
- A system of internal controls is functional and properly administered; and
- Practices comply with applicable policies and procedures.

To ascertain that objectives for the area under review are met and performance is monitored, we interviewed management and staff responsible for computer scheduling, monitoring software for building security and environmental equipment, and the reporting processes of the daily morning report and weekly status reports.

To determine policies and procedures are documented and adequate, we requested existing policy, procedure and standards manuals, and other written instructions concerning CSU activities and reviewed their scope and content.

To determine a system of internal controls is functional and properly administered, we conducted interviews with management and staff and observed work being performed.

To determine practices comply with applicable policies and procedures, we interviewed management and staff, reviewed existing policy, procedure and standards manuals, and observed work being performed.

Our audit was conducted in accordance with generally accepted government auditing standards and the Information Systems Audit and Control Association's IS Auditing Standards, and included such tests as we considered necessary in the circumstances.

Overall Evaluation

Based on our interviews and discussions, we conclude that CSU objectives are met and performance is monitored, policies and procedures are documented and operational, and internal controls are adequate, except for:

- Missing temporary access badges were not identified in a timely manner.

- The notification process for removing terminated employee access, especially contracted personnel, was rarely followed. Further, an ISS information technology security program that utilizes a continuous cycle for assessing, monitoring, and addressing risks has not been developed.

- Production Control processed software changes that could have a significant impact to County operations with only project leader authorization.

- The change control process does not address the role of the appropriately designated user representative.

- Software changes deemed to have a minimal impact on customers were implemented by Production Control without any supervisory approval. Additionally, a supplement to existing change management procedures confuses the definition of emergency software changes by requiring a change that simply needs a priority implementation schedule to be classified as an emergency change.

Additional opportunities for improvement were noted and are described herein.

RECOMMENDATIONS FOR IMPROVEMENT

RCC and Computer Room Access

1. Controls Over Temporary Access Badges Should Include a Review Process to Identify Missing Badges in a Timely Manner

Controls over temporary access badges are lacking a review process that would identify missing badges in a timely manner so corrective action could be taken. Our inventory identified two badges missing since November 2002.

Temporary badges are given to visitors of the RCC for their business related access (i.e., building service needs, maintenance activities, repairs, etc.). Before departing, the visitor is required to return the badge.

Although the badges are logged when given to visitors, there is no subsequent review of the log to assure all badges have been returned.

The badges provide access to the RCC and the computer room. Building access is compromised when temporary badges are not collected before the visitor leaves the premises.

We Recommend procedures be developed and implemented that assure the timely identification of missing temporary badges. All badges should be returned by the end of each day and any outstanding badges should be accounted for before the responsible employee leaves for the day. The status of those badges not returned the night before should be followed up on and reconciled promptly the next day. All discrepancies should be escalated to management for prompt corrective action.

Management's Response:

Concur. Formal process to be documented by May 20, 2004 to provide follow-up and reconciliation for badges not returned.

2. Access to the RCC, the Computer Room and Network Operations Center Should Be Restricted to the RCC Staff Required to Support Daily Operations

The computer room houses the hardware and accompanying software that provides various County services. Approximately 88 percent (135) of ISS's nearly 153 authorized positions have been granted unlimited access to the RCC. The majority of these individuals also have unlimited access to the computer room.

ISS employees are not required to log their arrival, departure, and reason for their visit. Therefore, management is unable to identify this irregular access. In addition, access to the computer room outside of a computer operator's routine work schedule is not logged.

We realize computer operators may need to work outside of their regularly scheduled work hours and access to the computer room by ISS personnel may be necessary. However, restricted access is required to assure continued availability of service and deter accidental or malicious actions. Segregation of duties controls are improved by limiting access to computing hardware.

Allowing excessive access to computer resources not only creates a distracting environment for the shift operators who monitor daily operations, but also exposes those assets to potential disruptions from accidental or malicious acts.

We Recommend:

A) Access to the RCC, the computer room, and network center should be restricted to the RCC staff required to support daily operations and RCC building access badge profiles should be adjusted accordingly based on each individual's assigned work schedule.

B) All work outside of regularly scheduled work hours be logged.

C) The access log should be periodically reviewed for questionable trends and escalated to management for corrective action when identified.

Management's Response:

A) Concur.

B) Concur. Formal process to be documented by May 20, 2004.

C) Concur. Formal process to be documented by May 20, 2004.

3. Access to the RCC Building and the Computer Room Contained Within Should Be Verified at Least Annually

The computer room houses the hardware and accompanying software that provides various County services. Access to the RCC building, and the computer room contained within, is not verified at least annually to determine the continued appropriateness of an individual's access.

Physical security is required in order to assure continued availability of service by limiting access that could result in accidental or malicious actions. In addition, segregation of duties controls is improved by limiting physical access to computing hardware.

Due to employee turnover, changes in daily responsibilities, job transfers, etc. RCC access may become unnecessary, resulting in excessive access to computer resources that expose those assets to potential disruptions from accidental or malicious acts.

We Recommend procedures be developed and implemented that establish and document the annual verification of individuals authorized to enter the RCC, the computer room and network center. The results of this

annual review should be used to update the existing "Physical Access to Computer Room" and "Employees Authorized to Access Computer Room" policies and guidelines. In addition, RCC building access badge profiles should be adjusted accordingly.

Management's Response:

Concur. Formal annual process to be documented by May 20, 2004.

Termination of Access

4. Security Administration Should Be Notified of Terminated or Transferred Personnel (Employees and Contractors) and User Access Should Be Periodically Re-Certified

Employees are granted access to various applications that reside on the mainframe or Unix servers based on their job responsibilities. In the case of Software Development and Technical Services, this may include the ability to change software. Access is also granted to contracted personnel that need access to the applications, but are not Orange County employees. There are approximately 200 contracted personnel with access to the mainframe.

We were informed by Security Administration staff that procedures are infrequently followed that require an employee's supervisor to notify Security Administration of terminated or transferred employees or contracted personnel that no longer require access. In addition, procedures have not been developed to periodically request user departments to re-certify their employees' access is appropriate.

After an employee is transferred or terminated, the employee's supervisor should notify Security Administration immediately so that access can be changed or removed as appropriate.

Some managers report terminated employees to the help desk or to the Security Administrator. As a detective control, Security Administration runs a report against Human

Resource data that lists employees that have been transferred or terminated. However, the report is not reliable.

Due to differences in the data compared, contracted personnel no longer requiring access are not identified in the report, all terminated employees listed in the report are not necessarily terminated, various IDs are listed as unidentified, and system service IDs also appear on the report. These anomalies require manual review and follow-up delaying the ID removal process.

Employees could have excessive access and/or multiple IDs when they transfer within the County or to/from elected officials and terminated employees may continue to have access to systems after they leave employment.

Contracted personnel that no longer require access create a significant risk because they are not identifiable from available reports.

We Recommend Security Administration develops and implements policies and procedures:

A) Requiring user management to notify Security Administration immediately upon employee termination or transfer;

B) To routinely advise user management of the need to promptly notify Security Administration of terminated or transferred employees and contracted personnel;

C) Periodically requesting user management review and re-certify user access, including contracted personnel, and confirm, based on access lists provided by Security Administration, that each user's access is appropriate based on their assigned job duties; and

D) To ensure that all contracted personnel are contractually required to adhere to County and ISS policies and procedures (including but not limited to internet usage, e-mail, security and confidentiality.)

Management's Response:

Concur. Existing policies will be modified and new ones added. Estimated completion date: July 30, 2004.

A) Concur. Policy being implemented. Estimated completion date: June 30, 2004.

B) Concur. Procedure being implemented. Estimated completion date: June 30, 2004.

C) Concur. Procedure being implemented with expected semi-annual review by user management and monthly review by security. Estimated completion date: October 29, 2004.

D) Concur. Policy and procedure being implemented. Estimated completion date: August 31, 2004.

Information Technology Security Program

5. An IT Security Program Should Be Developed

In 1999, the Security Administrator developed broad security guidelines. These general guidelines do not incorporate all of the required elements for a security program, nor have they been reviewed or approved by management or updated to address security concerns for specific applications and platforms. An IT security program has not been developed and communicated to the user community.

A security program should establish a framework and continuous cycle of activities for assessing risks, developing and implementing security procedures to address the risks, and monitoring the effectiveness of the procedures in addressing the risks. ISS management should also approve the security program at least annually.

Without a security program in place, responsibilities may be unclear, misunderstood, or improperly implemented. Sensitive or critical resources may be insufficiently protected and security expenditures and controls may be disproportionately or inconsistently applied.

We Recommend ISS management develops and implements a comprehensive security program that includes the continuous assessment of security risks and links the results of those assessments to existing policies and procedures to assure their continued effectiveness. Further, ISS management should review the security program annually to assure it remains in compliance with the County's goals and objectives.

Management's Response:

Concur. ISS management has implemented a security program that has been in effect for the last two years. This program will be linked to existing policies and procedures as requested and an annual review will be initiated. Estimated completion date: August 31, 2004.

Software Change Approvals

6. Request Forms for High-Risk Software Changes Should Be Submitted to the Production Control Supervisor After Approval by Appropriate Personnel

Software change control procedures refer to a committee that would meet to discuss and approve high-risk changes that affect a large number of users, or had the potential to affect a large number of systems. The committee included the equivalent to the current CIO, Unit Supervisors and the Change Coordinator, but has been disbanded for approximately two years.

We were informed Production Control has been processing high-risk software changes with only project leader authorization.

High-risk changes require supervisory approval through all phases of the project. The appropriately designated user representative is required to approve, test, and accept for production implementation all changes that impact their application.

High-risk changes to production applications create a risk to customer service levels and to production data from errors and omissions.

We Recommend a completed change request form be submitted to the Production Control Supervisor with appropriately designated user representative and Systems Development Unit Supervisor approvals prior to the implementation of high-risk software changes to production applications.

Management's Response:

Concur. User representation and Systems Development approvals are being planned for implementation of Change Management software in the second quarter of 2004.

7. Request Forms for Routine Software Changes Should Be Submitted to the Production Control Supervisor After Approval by Appropriate Personnel

ISS has established procedures for routine changes that are defined as various system and application internal table updates, ad hoc reporting, and minor maintenance with minimal impact on customers that have back-out procedures in place.

Routine software changes do not require approval prior to production implementation. Further, routine changes are not listed separately in management reports. We found that as many as 13 routine changes were completed in a week.

According to the "Orange County Information Systems and Services Standards and Policies Manual", the change developer's project leader is responsible for certifying that the change is ready to be installed.

The appropriately designated user representative (system owner) is required to approve, test, and accept for

production implementation all changes that impact their application.

Routine software change procedures have been designed for a fast-track implementation of changes, but in the process have circumvented required controls. Any changes to production applications create a risk to customer service levels and to production data from errors and omissions.

We Recommend a completed change request form be submitted to the Production Control Supervisor with appropriately designated user representative and project leader approvals prior to routine software changes being implemented to production applications.

Management's Response:

Concur. User representation and Systems Development approvals are being planned for implementation of Change Management software in the second quarter of 2004.

8. Emergency Software Change Procedures Should Be Followed for Changes That Are in Fact the Result of True Emergency Conditions. Changes Requiring Priority Implementation Should Not Be Classified as Emergency Changes

We reviewed an emergency software change and noted that a problem report was never created that would identify the problem being corrected. We subsequently learned the change was categorized as an emergency only because the developer required the change to be installed as soon as possible instead of the standard time frame established by change control procedures.

Further, the change request form for this change was completed and submitted to Production Control by the developer and the change was installed even though the change request did not have the required approval.

We reviewed several weekly reports and found that approximately seven emergency changes are being completed a week.

According to the ISS Standards and Policies Manual the definition of emergency changes are changes resulting from "…problems in which there is a critical impact on a customer caused by an unusable system, component or procedure and there is no alternative available…". The manual also states that emergency changes require, "…a problem record…" and "…be approved by developer's unit supervisor, or designee in the absence of unit supervisor…".

Further, emergency changes only require a verbal approval for the change to be implemented and the required change request form is supposed to be submitted by the following day with appropriate approvals.

In 1995 a supplement to existing change management procedures was issued that contained a reminder that if the established standard time frames for implementing software changes, "…cannot be met then your Change Request should be submitted as an emergency…".

We believe this reminder confuses the definition of emergency software changes by requiring changes that merely shortcut established standard implementation time frames be considered emergency changes.

Emergency software changes are necessary to resolve unexpected processing problems in a timely manner. The documentation and approval of these changes typically occurs after the change has been made. As a result, software change controls are circumvented when this type of change is made. This condition exposes production application libraries to unauthorized changes that may result in future application failures or erroneous production data.

Additionally, when software changes are misclassified, the risks associated with emergency changes are not identifiable to ISS management. In addition, problem trends cannot be identified and development staff with responsibility for the

application involved may not be adequately informed of the problems.

We Recommend emergency software change procedures be followed for changes that are in fact the result of emergency conditions. In addition, Production Control personnel should ensure that appropriate approvals are obtained for all emergency changes and that problem reports have been included in change documentation. Further, procedures should be developed and implemented for changes requiring priority implementation schedules and they should conform to regular change control procedures.

Management's Response:

Concur. Appropriate approvals are being planned for emergency changes with the implementation of Change Management software in the second quarter of 2004. In addition, incident report association is also being planned.

9. Software Change Control Procedure Manuals Should Be Updated

There are two manuals distributed to all ISS personnel. One is a specific "how-to" manual for using one of the change control software products that has not been updated since 1990. The other is the "Orange County Information Systems and Services Standards and Policies Manual" that was last updated in August 2000.

The latter manual includes procedures to follow for submitting a request, authorization requirements, and responsibilities for individuals involved in the change management process. Some of the processes have significantly changed for example, there was a committee that met to discuss and approve high-risk changes that affect a large number of users, or had the potential to affect a large number of systems. The committee has been disbanded for approximately two years.

Software change control procedures have significantly changed and neither of the two subject manuals have been updated. We also identified that Harvest, the application used for Unix and NT changes, is not included in either of the manuals.

Policies and procedures should be updated with current information reflecting management's requirements and approved operating practices. Policies and procedures provide direction and control for users that are initiating a change and for personnel performing the change.

Outdated policies may result in noncompliance with management requirements and unintended consequences. The value of the manual as a reference is diminished if the procedures are not kept up to date.

We Recommend ISS management periodically reviews and updates policies and procedures to ensure they are current and conform to management's established directives.

Management's Response:

Concur.

Security Violation Reports

10. User Management and Security Administration Should Review Security Violation Reports

IBM's Resource Access Control Facility (RACF) software is used to provide mainframe access control. RACF automatically provides security violation reporting, although Security Administration is not generating these reports. As a result, user management and Security Administration do not review violations.

Security Administration and user management should be reviewing security violation reports to identify attempts to circumvent security controls and identify unauthorized users trying to gain access to the system and data.

Security Administration stopped generating the reports because IDs are locked out after three unsuccessful attempts to access the mainframe.

We feel however, that without a documented review of security violation reports, user management and Security Administration cannot identify and take appropriate action on all unauthorized attempts to access the mainframe or data.

We Recommend Security Administration distributes security violation reports to appropriate User Management for follow-up and resolution of identified violations.

Management's Response:

Concur. Procedure being implemented. Estimated completion date: July 30, 2004.

Excessive Access Privileges

11. Privileges and Access to CA Scheduler Software Should Be Limited to Appropriate Personnel

ISS users can log-on to the application, CA Scheduler, to schedule jobs for daily/weekly/monthly/annual processing on the mainframe. A user with manager privileges, the highest authority level, is allowed to define new User IDs, control all schedules and jobs, and issue purge commands.

There are twenty-one IDs that have manager privileges, which in the majority of cases are excessive for their job responsibilities. Seven are assigned to individual users (four Production Control and three Technical Services), and fourteen are used by applications to automatically initiate jobs without user intervention.

Access to applications should be limited to those people that require access to perform their job duties. In addition, administrative responsibilities should be restricted to limit risk inherent with this level of access.

Access was granted to technical services personnel so that they could perform application troubleshooting and

maintenance on the application during or subsequent to an upgrade.

An ID with manager privileges could be used to make changes to the job schedule. Assigning excess privileges increases the risk of inadvertent changes and malicious acts.

We Recommend:

A) Access to CA Scheduler be restricted to Production Control and Computer Operations personnel as required to perform their job responsibilities.

B) Manager privileges to CA Scheduler be limited to two people within Production Control; the person assigned the responsibility for adding users and their backup.

Management's Response:

A) Concur.

B) Concur. Three individuals are assigned Manager privileges for the product due to position requirements.

Unique User IDs and Passwords

12. CA Scheduler Users Should Be Assigned Unique User IDs and Passwords for System Access

ISS users can log on to CA Scheduler to schedule jobs for daily/weekly/monthly/annual processing on the mainframe. Each user is assigned a User ID and has to enter a READ and/or WRITE password to access CA Scheduler. Although an ID is required to sign-on to the mainframe, the same ID does not have to be entered to access CA Scheduler. The User IDs are created using a commonly known design, making it easy for users to identify another's ID, and the same password is assigned to all users. There were 27 operators that share the same read and write passwords. Four production control personnel share a different password.

Users should be assigned unique user IDs and passwords to gain access to all applications. IDs can be generally known among users, but each user should know only their own password.

For this system, administrators assign both the ID and the password. Even though they have the capabilities within the system to assign individual passwords, they are assigning one Read and Write password for all users.

Accountability for actions performed on automated systems is eliminated when users can log-on using another person's ID. Further, this weakness enables users to gain an increased level of access to the system. It should be noted that due to a weakness in this system, there will be two people, the user and the administrator, that could use the assigned ID and password combination.

We Recommend each CA Scheduler user be assigned a unique User ID and password.

Management's Response:

Concur.

Contract Administration

13. The ISS Contract Administrator Should Maintain the Annual Maintenance Agreement for All Equipment

The ISS Contract Administrator could not provide the annual maintenance agreement with the EMC Corporation for the Storage Area Network System (SANS) prior to completion of fieldwork.

The maintenance on this hardware, which stores mission critical data, is performed over a dial-up connection by EMC. Although there are procedures for the computer operators to follow when EMC makes a request for this access, the roles, responsibilities, and extent of liability could not be determined since the maintenance agreement was not available for review.

All maintenance agreements should be on-hand for reference by ISS personnel. The agreements should outline equipment covered, services provided, response time for support, and responsibilities for all parties covered by the agreement.

Enforceable service agreements that define roles and responsibilities and that evidence concurrence by all parties involved in the agreement are especially critical when the vendor can make remote changes to equipment that houses mission critical data.

We Recommend ISS personnel:

A) Assures all maintenance agreements are on-hand for reference;

B) Obtains and reviews the agreement with EMC Corporation to assure authorization requirements, confidentiality and proficiency of technical staff are addressed;

C) Ensures that all future vendor agreements require vendor adherence to County and ISS policies and procedures (including but not limited to internet usage, e-mail, security, confidentiality, etc.); and

D) Ensures that all future vendor agreements include provisions for security responsibilities and procedures.

Management's Response:

A) Concur.

B) Concur.

C) Concur. Procedure being implemented. Estimated completion date: August 31, 2004.

D) Concur. Procedure being implemented. Estimated completion date: August 31, 2004.

14. CSU Personnel Should Verify That Maintenance Is Being Performed According to the Agreed-Upon Schedules

The CSU has several preventative maintenance contracts with different vendors to provide maintenance on the environmental control systems including the generator, uninterruptible power supplies, power distribution units, air conditioning (A/C), and fire suppression systems. They also have a preventative maintenance contract for the printers. In addition, the vendors perform testing on each of these systems as part of this maintenance.

Each of the contracts has a different schedule of maintenance; the agreements range from weekly to annually. CSU personnel do not have copies of the contracts outlining the maintenance required to be performed and do not verify that the maintenance is being performed according to the agreed upon schedules. During a scheduled floor cleaning, the vendor found that the A/C filters were very dirty. Although CSU personnel reacted to the floor cleaning inspection, this condition occurred because the routine preventative maintenance was not being performed.

Preventative maintenance should be performed according to a predetermined schedule. CSU personnel are responsible for ensuring that the required maintenance is performed according to the schedule.

CSU personnel indicated that it is the vendors' responsibility to ensure that preventative maintenance is being performed in a timely manner according to the predetermined schedule.

If preventative maintenance is not performed, this could lead to a failure of one of the environmental control systems, which could result in a disruption of service. Not performing preventative maintenance also shortens the useful life of the equipment.

We Recommend CSU personnel establishes procedures to ensure that preventative maintenance is performed

according to contractual arrangements and defined schedules.

Management's Response:

Concur. Formal process to be documented by May 20, 2004.

15. CSU Personnel Should Maintain a List of Equipment and Reconcile Hardware Covered Under Maintenance Agreements

Orange County entered into a hardware maintenance contract with IBM for the period of June 1, 2002 through May 31, 2005. The monthly amount, approximately $24,000, is based on a schedule of costs included in the contract. At the time of the contract negotiation, CSU personnel reviewed their inventory and determined which equipment to include in the contract. We were informed that when new equipment is added, the contract liaison notifies the vendor verbally of the change during their monthly meeting. However, CSU personnel do not receive or maintain a list of the equipment that could be used to verify the hardware covered by the maintenance agreement. Additionally, the vendor is supposed to provide an inventory to CSU Personnel quarterly. The contract liaison has not received a list since the contract was signed, nor have CSU personnel requested a copy from IBM.

According to the contract, "…The County will provide written notification of equipment removed from coverage…" and "…On a quarterly basis, the Vendor will provide the County with a complete, comprehensive listing of all equipment under maintenance…".

The contract liaison is responsible for ensuring an accurate equipment inventory and that obsolete inventory is not included in the monthly maintenance price.

The County could be paying excess fees for maintenance on equipment that is not being used. There could also be new

inventory that has not been added to the maintenance contract. If the equipment failed, it would not be covered under the maintenance contract.

We Recommend CSU personnel:

A) Obtains a current listing of the equipment covered under the IBM maintenance contract and reconcile it with the current inventory;

B) Updates or establishes procedures for the timely notification of additions and deletions to maintenance contracts; and

C) Updates or establishes procedures to review and reconcile vendor-supplied quarterly reports.

Management's Response:

A) Concur.

B) Concur.

C) Concur.

Service Level Agreements

16. Service Level Agreements Should Be Established, Agreed To, and Documented for All Major User Groups

Service level agreements that set system availability, response time, and job turnaround targets have not been established, agreed to, or documented for all major user groups.

According to management, the sole service level agreement in effect was with Corrections, the only twenty-four hour seven days a week customer. We reviewed the service level agreement that was dated 1992, and noted it was not approved by any of the parties to the agreement and "ROUGH DRAFT" was notated at the bottom of each page.

In addition, the agreement had references to a system, "IBM Office Vision", no longer in use by the County.
A common understanding between provider and user regarding the level of service required and the formalization of the performance criteria against which the quantity and quality of service will be measured needs to be established.

Not establishing agreed upon service level targets may result in unreasonable expectations by users of services. Conversely, the lack of performance measurement criteria may result in missed opportunities to identify problems causing low service levels.

We Recommend:

A) Service level agreements, that establish system availability, response time, and job turnaround targets, should be established, agreed to and documented for all major user groups.

B) A periodic review of agreements in effect should be performed to assure they are maintained in a current fashion.

C) The service level agreement with Corrections should be updated, re-negotiated, and formalized.

Management's Response:

A) Partially concur. ISS generally recognizes the advantages of formal service level agreements with customers. It is further recognized that close working partnerships with identified resources, project plans, and delivery goals can be equally effective. The ISS enterprise support model is simply stated; "24X7" support and service. Service level agreements for services will be developed for elected officials and constitutional officers, particularly where ISS is providing specific and/or limited services such as infrastructure support for the Public Defender.

B) Partially concur. We've found that ISS maximizes services to other County departments through direct and constant communication rather than service level agreements with other entities in the organization.

C) Partially concur. We've found that ISS maximizes services to other County departments through direct and constant communication rather than service level agreements with other entities in the organization.

Project Performance Measurement

17. Project Milestones and Deliverables Should Be Measured, Evaluated and Corrective Action Implemented Where Necessary

The achievement of objectives, specifically costs and time, for major ISS projects is not measured. Although project software is used to track the start and finish dates and percent complete for each of the individual required tasks within the Enterprise Backup project, there have been no comparisons of planned costs and time to actual and estimated future costs and time for the overall project.

Project management identifies cost and time overruns early on so corrective action, if necessary, can be taken in a timely manner.

The current tracking of the project is only at the task level and reporting includes a start date, finish date, and a percent complete. There is no tracking of expenditures and planned completion timeframes.

Without the ability to identify cost and time overruns early on corrective action may be delayed, negatively impacting project costs and schedules for the particular project and the schedule for subsequent projects.

We Recommend management measures the achievement of objectives for major ISS projects. Specifically, project milestones and deliverables that include cost and completion timeframes should be measured, evaluated, and corrective action implemented where necessary.

Management's Response:

Concur. Product Administration database currently being modified to formally track this information. Implementation scheduled in the next six (6) months.

Evidence of Project Approval

18. Documented Management Approval Should Be Obtained for Projects Before Committing Funds and Resources

Documented ISS management approval for the Enterprise Backup project, estimated cost of $443,000, was not available.

According to management, the savings from not renewing licenses for the existing backup process that involved various vendors and hardware offsets the costs associated with this project. However, documentation evidencing this analysis was not available.

Project approval at an appropriate management level validates the commitment of funds and resources, and evidences management's understanding of the impact of a project on both the ISS Division's financial and staffing resources. In addition, the approval establishes the project's base line requirements.

We Recommend cost comparisons be prepared and documented for significant projects. In addition, appropriate management approval should be obtained and documented for projects undertaken by ISS before committing funds and resources.

Management's Response:

Concur. We currently follow Orange County Purchasing processing and procedures for acquiring hardware and software. In addition, we are continuing to make our internal ISS purchasing processes more robust.

Requisition Approvals

19. Approvals Should Be Obtained and Documented before Purchase Requisitions Are Processed

Of eight purchase orders (PO) totaling $142,000 and relating to hardware, software, and contract expenses, none had authorization by the Division's own standard of e-mails, signed quotes, or meeting minutes.

Within the above sample, no supporting documentation could be provided for one PO.

According to the Purchasing Procedure manual, "all requisitions shall be authorized by the Department Head/Division Head or designated authority." Additionally, approval is required to assure the appropriate level of management is involved in the transaction and asserts to the transaction's validity.

Without documented evidence of approvals, compliance to purchasing requirements is not supported and accountability cannot be effectively determined thereby negatively impacting the transaction's audit trail.

We Recommend procedures be developed and implemented that require documented approval before the purchase requisition data is forwarded to the Purchasing and Contracts Division. If purchasing authority is delegated by the Division Head, it should be documented as to who has the authority, the limits of authority and the duration of the authority. The person preparing the requisition should use this information to verify purchase requests have been properly authorized. In addition, supporting documentation should be retained that provides evidence of the substance of the transaction as well as its approval.

Management's Response:

Concur.

20. Purchase Orders Should Be Processed with the Correct Sources of Funds

Although later corrected, we noted that a PO had incorrect sources of funds. The account, "Software Under $750" was charged $20,000 for software that had unit costs of $833 and $1,666.

According to the Purchasing Procedure manual, the department that prepares purchase requisitions should "Verify that all sources of funds identified on the requisition are properly coded as to department/division and object code." In addition, Generally Accepted Accounting Principles (GAAP) require expenses be categorized correctly.

Errors in selecting the source of funds reduce the effectiveness of budget controls that could result in funding shortfalls for planned purchases.

We Recommend a procedure be established and implemented that assures the accuracy of sources of funds used in purchase requisitions electronically submitted to the Purchasing and Contracts Department.

Management's Response:

Concur.

Security Risk Assessment

21. A Formalized Risk Assessment That Establishes a Required Level of Security Should Be Performed

A formalized risk assessment that establishes a required level of security has not been performed.

Management should conduct and periodically update a comprehensive risk analysis to determine the security threats to the data and information technology resources.

Although not formalized in a risk assessment, during the planning and construction of the RCC various physical risks

were identified and efforts put forth to reduce or eliminate their impact to the operations of the CSU and consequently to the internal and external customers they serve. However, similar considerations relating to the more intangible type of security, for example, identification of sensitive data, adequacy of access levels to sensitive applications and data including program libraries, potential exposures resulting from access by external sources, virus protection needs, the adequacy of access control lists, etc., has not been performed.

Without risk analyses being performed, inappropriate levels of access could be granted to users, and gaps in security or areas that require additional security may be unsecured because they have not been identified.

We Recommend ISS management:

A) Performs and documents a formal risk assessment, for all functions within ISS and implements and documents a level of security commensurate with the risks identified;

B) Develops and implements procedures to update risk assessments as changes occur; and

C) Develops and implements procedures that require an annual review of risk assessments to assure a continued level of adequate security.

Management's Response:

A) Concur. Procedure being implemented. Estimated completion date: October 29, 2004.

B) Concur. Procedure being implemented. Estimated completion date: October 29, 2004.

C) Concur. Procedure being implemented. Estimated completion date: October 29, 2004.

Security Awareness

22. Security Guidelines, Procedures, and Responsibilities Should Be Routinely Communicated to Users

Security responsibilities are not periodically communicated to users and Security Administration does not routinely provide employee training regarding security risks, roles and responsibilities.

For security guidelines and procedures to be effective, they should be communicated to the user community. Security awareness training should also be held periodically for all employees to assure timely information distribution and to emphasize the importance of security.

Security Administration has developed various media including videos and brochures; however, this information has not yet been distributed to employees.

Users should be aware of their responsibility for protecting their user IDs and passwords from compromise. If they are not informed of all their responsibilities regarding security, it increases the likelihood that an unauthorized individual could gain access to a system.

We Recommend security guidelines and procedures be routinely communicated to the user community and that periodic security awareness training be conducted for current and newly hired employees.

Management's Response:

Concur. Procedure being implemented. Estimated completion date: October 29, 2004.

23. The ISS Policies and Procedures Manual Should Be Updated

The ISS Policies and Procedures Manual includes a section on security and integrity that was developed in 1995 as a

guideline for the mainframe environment and has not been updated to address Windows and Unix security.

In addition, procedural changes have not been included in the manual. For example, all requests for access, security changes, and password problems are now sent to the User Help Desk before being forwarded to Security Administration for verification that appropriate personnel are initiating the request. Help desk personnel also perform password resets without consulting Security Administration.

Policy manuals should accurately reflect management's current policies and procedures. As an aid to communicate management's commitment to security, and to evidence the program as an authoritative reference, policies should be approved annually.

Without current and clearly stated security policies and guidelines in place, confusion regarding security responsibilities, by both users and the help desk, may result in exposure of County data to unauthorized access.

We Recommend ISS management:

A) Reviews and updates security policies and procedures to reflect currently approved operating procedures; and

B) Reviews and approves the section addressing security and integrity at least annually.

Management's Response:

A) Concur. Procedure being implemented. Estimated completion date: October 29, 2004.

B) Concur. Procedure being implemented. Estimated completion date: October 29, 2004.