County of San Diego Auditor and Controller

OFFICE OF AUDITS & ADVISORY SERVICES

COMPUTER OPERATIONS AUDIT

FINAL AUDIT REPORT

Chief of Audits: James L. Pelletier, CIA, CICA
IT Audit Manager: Lynne Prizzia, CISA
Senior Auditor: Mady Cheng, CPA, CISA
Auditor II: Evans Owala, CISA

Report No. A09-045

October • 2010

Intentionally Left Blank

DONALD F. STEUER
CHIEF FINANCIAL OFFICER
(619) 531-5413
FAX (619) 531-5219

County of San Diego

AUDITOR AND CONTROLLER
1600 PACIFIC HIGHWAY STE 166, SAN DIEGO, CALIFORNIA 92101-2478

TRACY M. SANDOVAL
ASST. CHIEF FINANCIAL OFFICER/
AUDITOR & CONTROLLER
(619) 531-5413
FAX (619) 531-5219

October 1, 2010

TO: W. Harold Tuck, Chief Information Officer
County Technology Office

FROM: James L. Pelletier
Chief of Audits

FINAL REPORT: COMPUTER OPERATIONS AUDIT

Enclosed is our report on the Computer Operations Audit. We have reviewed your responses to our recommendations and have attached them to the audit report.

The actions taken and/or planned, in general, are responsive to the recommendations in the report. As required under Board Policy B-44, we respectfully request that you provide quarterly status reports on the implementation progress of the recommendations. The Office of Audits & Advisory Services will contact you or your designee near the end of each quarter to request your response.

Also attached is an example of the quarterly report that is required until all actions have been implemented. To obtain an electronic copy of this template, please contact Mady Cheng at (858) 495-5679.

If you have any questions, please contact me at (858) 495-5661.

JAMES L. PELLETIER
Chief of Audits

AUD:MC:aps

Enclosure

c: Mikel D. Haas, Deputy Chief Administrative Officer, Community Services Group
Donald F. Steuer, Chief Financial Officer
Tracy M. Sandoval, Assistant Chief Financial Officer/Auditor and Controller
April Heinze, Director, General Services
Susan L. Green, Assistant Chief Information Officer
Ebony N. Shelton, Group Finance Director, Finance and General Government Group
Kaye Hobson, Group Finance Director, Community Services Group

INTRODUCTION

Audit Objective

The objective of the audit was to evaluate the design and operating effectiveness of the internal controls surrounding the County's computer operations.

Background

Computer operations is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities.

Data Centers and Server Rooms – As of November 2009, the Northrop Grumman Team (NGT) supported the County's 602 computer servers and 455 active applications. There were 169 servers in various sites throughout San Diego County, and the remaining servers resided in two primary Hewlett-Packard (HP) data centers in Tulsa, Oklahoma and Plano, Texas. NGT is responsible for the physical and environmental security of its facilities, including the AT&T Data Center in San Diego and the two primary HP data centers.

Similarly, the County is responsible for the security of its own facilities. The Electronic Security Division of the Office of Security Services of the Department of General Services (DGS) uses the Card Access System to manage photo identification/access cards (Access Cards) which grant cardholders access to enter County facilities, including server rooms. In addition, the Sheriff's and the Probation Departments manage the Access Cards for their own staff. Within the Card Access System, physical access is assigned by Access Group. In particular, various Access Groups are set up in the Card Access System, each Access Group is granted physical access to specific County facilities, and each Access Card is assigned up to six Access Groups.

Job Scheduling – The NGT Application Service framework team schedules and manages IT jobs using job scheduler software. Job schedulers are a major component of the County's IT infrastructure and manage the County's production workload on mainframe, Windows, Unix, AS400, and VAX platforms.

Incident and Problem Management – The NGT Help Desk Service framework team manages trouble tickets and service requests from inception to closure (i.e., recording, troubleshooting, escalating, coordinating, reporting, and closing). Incidents reported are tracked in the Peregrine ticketing application. According to the Deputy Infrastructure Operations Manager of Northrop Grumman (NG), upon closing high-priority incident tickets (i.e., Severity 1 and 2), NGT performs root cause analysis to prevent recurring problems.

Audit Scope & Limitations

Audit fieldwork was conducted between June 2009 and February 2010. The audit focused on the following areas of computer operations:

- Physical and environmental security of the County's server rooms in San Diego;
- Job scheduling and controls in Windows and Unix platforms;
- Incident and problem management;
- Deliverables and reports as specified in the IT Contract; and
- Backup and restoration.

The Office of Audits & Advisory Services' (OAAS) ability to audit backup and restoration was limited due to the contractor's inability to provide requested documentation. OAAS plans to revisit these areas in a future audit.

This review was conducted in accordance with auditing standards prescribed by the Institute of Internal Auditors, Inc., as required by California Government Code, Section 1236. OAAS also based the evaluation on standards related to information technology security controls from the IT Governance Institute's *Control Objectives for Information and Related Technology* (COBIT) and National Institute of Standards and Technology's (NIST) *Recommended Security Controls for Federal Information Systems*.

Methodology

Key components of OAAS' approach to conducting the audit are highlighted below:

- Interviewed selected NGT and County personnel, including Group IT Managers (GITM's), on policies, processes, and procedures relevant to the areas being reviewed. Obtained and evaluated related documents;

- Researched and reviewed the *IT and Telecommunications Service Agreement* between the County and NG (IT Contract);

- Conducted site visits in three sample server rooms (the AT&T Data Center, County Administration Center [CAC], and Mills Building) to observe and verify existence and appropriateness of physical access and environmental controls (e.g., existence of fire suppression system);

- Inquired the DGS staff about the process of managing Access Cards. Obtained and reviewed the list of individuals with access to the CAC server room to evaluate appropriateness (e.g., to identify users with duplicate Access Card accounts and/or any terminated County or NGT employees);

- Identified key job scheduling controls and performed detailed testing;

- Walked through the incident and problem management process with NG personnel and tested key controls; and

- Tested sample deliverables/reports from the IT Contract to verify whether the NGT provided the reports to the County.

Audit Results

Summary

Within the scope of the audit, OAAS concluded that controls over computer operations were generally adequate, except for the following opportunities for improvement in disaster recovery, server room access management, and job scheduling.

Finding I:

AT&T Data Center Needs an Approved Disaster Recovery Plan

As of the end of audit fieldwork, there was no approved disaster recovery plan for the AT&T Data Center. CTO management stated that while NGT has a plan for the site, the plan does not meet the County's requirements and therefore has not been approved by the CTO. As of November 2009, the AT&T Data Center housed 35 County servers, including critical infrastructure and application servers. An alternate processing site or telecommunication services to support the recovery of County information systems and network infrastructure in the event of a disaster had not been identified.

If a disaster (e.g., firestorm, earthquake, or terrorist attack) occurs, the computer equipment and systems housed in the AT&T Data Center may be destroyed or severely damaged. Without an alternate processing site or a backup telecommunication service, the County would be unable to restore certain critical IT systems and the County's primary network, and could not resume related business functions in a timely manner.

A comprehensive disaster recovery plan is required to ensure that business functions can be timely resumed in the event of a critical system or network failure.

Recommendation:

The County Technology Office (CTO) should work with the NGT management to develop and implement a disaster recovery plan for the AT&T Data Center. As this could result in significant costs to the County, the disaster recovery plan should be based on a business impact analysis conducted to assess potential impact to County operations in the event of a disaster.

Finding II:

Access Management to CAC Server Room Needs Improvement

In November 2009, the CAC server room housed 12 County servers. OAAS tested the list of personnel with access to the CAC server room as of May 2009. The following issues were identified:

Inappropriate Access Granted – There were 299 active Access Card accounts which provided physical access to the CAC server room. These 299 accounts were composed of 132 Sheriff employee accounts, 94 other County employee accounts, 70 NGT accounts, and three other contractor accounts. Thirty-one of the 299 Access Cards (10%) had never been used. Additionally, 11 County executives and two gardeners whose job responsibilities did not require the access had access to the server room.

Terminated NGT Employees – Five of 64 active accounts sampled represented terminated NGT employees whose 24/7 access to the server room had not been removed from the Card Access System. According to the DGS Electronics Security staff, the five Access Cards had never been returned to DGS. OAAS was able to verify that four of the five cards had not been used after the employee was terminated. The termination date for the fifth employee was not available.

According to the County Administrative Policy #0040-6, each department is responsible for collecting Access Cards from contractors who leave County services, and Access Cards will be returned to the DGS Security Office for destruction. However, there was no process to ensure NGT staff's Access Cards were returned to DGS upon termination. Also, there were no formal procedures for communication of NGT staff termination to the DGS Electronics Security Division. In addition, NGT only provided the list of terminated employees upon DGS' request and as a result, access removal had been sporadic and delayed.

County Employees with Multiple Access Card Accounts – Six County employees had multiple active accounts in the Card Access System and each related Access Card allowed the cardholder to access the CAC server room. The six employees accounted for 18 of the 165 accounts sampled (11%).

If Access Cards are not properly managed, physical security at County facilities could be compromised. Unauthorized personnel could gain physical access to restricted areas such as server rooms and damage computer equipment or data, resulting in breach of confidential information, misappropriation of assets, and/or identity theft.

Recommendation: The CTO management should work with the DGS to strengthen physical access controls to County server rooms, including the CAC server room. This should include, but not be limited to:

- Establishing a new Access Group in the Card Access System so that only this new Group is allowed to access the CAC server room. Access to the CAC server room should be removed from all other Access Groups. Requests to join this new Group should be approved by the CTO;

- Working with the NGT management to develop and implement procedures to ensure that the access of NGT staff no longer working on the County contract is removed and related Access Cards are collected and returned to DGS in a timely manner; and

- Working with the NGT and County departments to review the list of personnel with access to County server rooms at least semi-annually to identify:
  - Terminated employees/contractors;
  - Personnel with multiple Access Card accounts; and
  - Personnel whose job responsibilities do not involve accessing the server rooms on a regular basis.

  Any inappropriate access identified should be immediately removed.

Finding III: **Job Scheduling Process Needs Improvement**

Job scheduling procedures were incomplete, not formally documented, and/or not properly reviewed and approved. As a result, all nine samples of new jobs added to the production environment lacked evidence of County management approval. Also, the NGT had never produced or provided the County with the *Servers Job Scheduling Requirements Report*, as required by the IT Contract.

The COBIT framework states that complete and accurate data processing requires effective management of data processing procedures, including defining operating policies and procedures for effective management of scheduled processes. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.

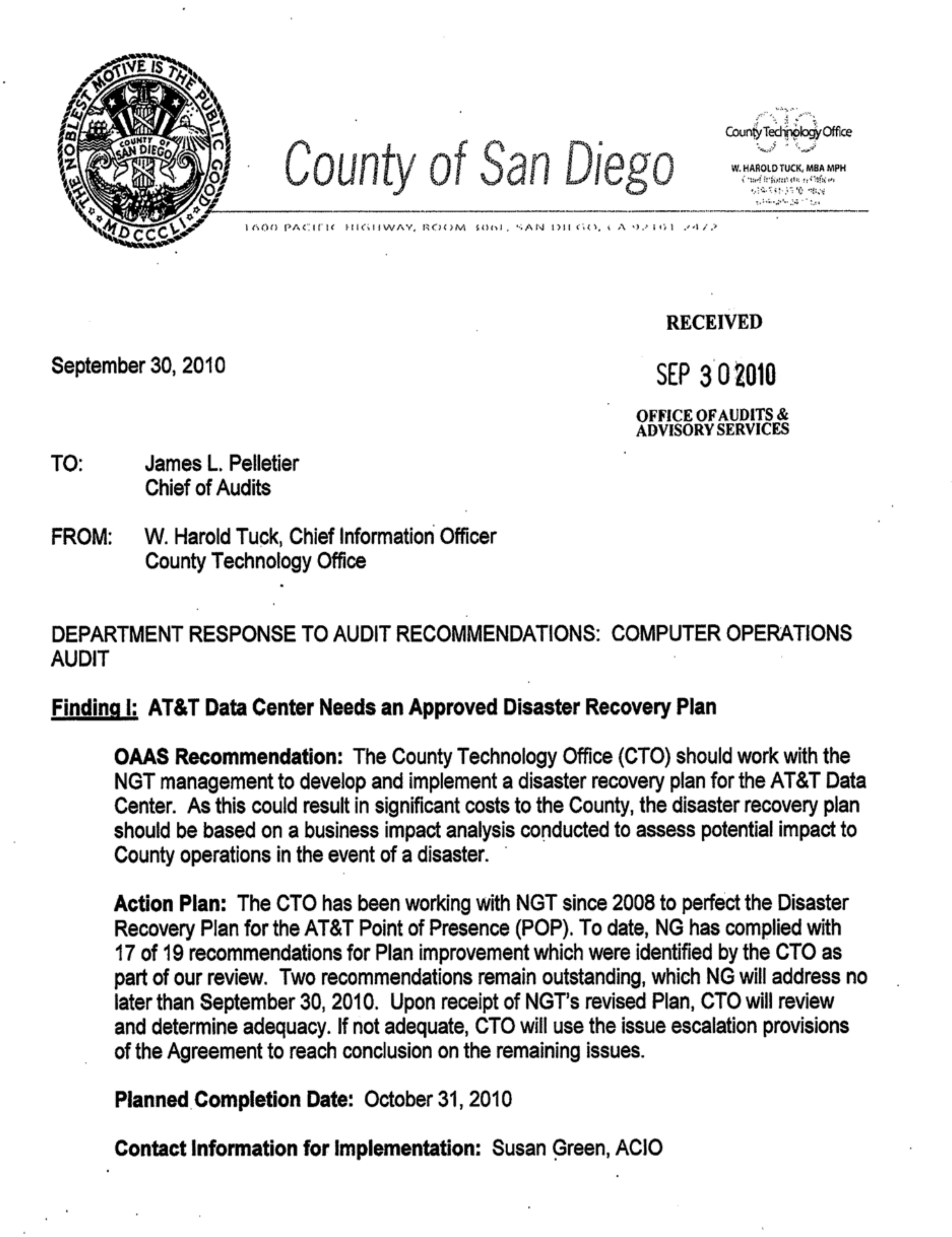
Unauthorized jobs could potentially be added to the production environment, resulting in unauthorized changes to the application and/or data. Consequently, data integrity could be compromised, resulting in a potential breach of confidential information, misappropriation of assets, and/or identity theft.

Recommendation: The CTO and the NGT management should develop, update, review, approve, and implement the job scheduling procedures for all platforms processing County jobs. New or changed jobs should be properly approved and supporting documents should be retained in compliance with the County's records retention policies.

COMMENDATION

The Office of Audits & Advisory Services commends and sincerely appreciates the courteousness and cooperation extended by the officers and staff of the County Technology Office, the Department of General Services, and the Northrop Grumman team throughout this audit.

DEPARTMENT'S RESPONSE



County of San Diego

County Technology Office

W. HAROLD TUCK, MBA MPH
Chief Information Officer
[illegible]
[illegible]

1600 PACIFIC HIGHWAY, ROOM 306, SAN DIEGO, CA 92101-2472

September 30, 2010

TO: James L. Pelletier
Chief of Audits

FROM: W. Harold Tuck, Chief Information Officer
County Technology Office

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: COMPUTER OPERATIONS AUDIT

Finding I: **AT&T Data Center Needs an Approved Disaster Recovery Plan**

OAAS Recommendation: The County Technology Office (CTO) should work with the NGT management to develop and implement a disaster recovery plan for the AT&T Data Center. As this could result in significant costs to the County, the disaster recovery plan should be based on a business impact analysis conducted to assess potential impact to County operations in the event of a disaster.

Action Plan: The CTO has been working with NGT since 2008 to perfect the Disaster Recovery Plan for the AT&T Point of Presence (POP). To date, NG has complied with 17 of 19 recommendations for Plan improvement which were identified by the CTO as part of our review. Two recommendations remain outstanding, which NG will address no later than September 30, 2010. Upon receipt of NGT's revised Plan, CTO will review and determine adequacy. If not adequate, CTO will use the issue escalation provisions of the Agreement to reach conclusion on the remaining issues.

Planned Completion Date: October 31, 2010

Contact Information for Implementation: Susan Green, ACIO

Finding II: Access Management to CAC Server Room Needs Improvement

OAAS Recommendation: The CTO management should work with the DGS to strengthen physical access controls to County server rooms, including the CAC server room. This should include, but not be limited to:

- Establishing a new Access Group in the Card Access System so that only this new Group is allowed to access the CAC server room. Access to the CAC server room should be removed from all other Access Groups. Requests to join this new Group should be approved by the CTO;
- Working with the NGT management to develop and implement procedures to ensure that the access of NGT staff no longer working on the County contract is removed and related Access Cards are collected and returned to DGS in a timely manner; and
- Working with the NGT and County departments to review the list of personnel with access to County server rooms at least semi-annually to identify:
  - Terminated employees/contractors;
  - Personnel with multiple Access Card accounts; and
  - Personnel whose job responsibilities do not involve accessing the server rooms on a regular basis.

  Any inappropriate access identified should be immediately removed.

Action Plan: CTO and DGS are currently working to eliminate all unnecessary employees from having access to the 9th floor of the CAC. Included in these actions are:

- ○ A new Access Group has been established and is being populated with only those individuals who need access to the 9th floor.
- ○ NGT is scrubbing the list of terminated employees and ensuring that their Access Cards have been deactivated.
- ○ CTO and NGT will review, semi-annually, the list of personnel with access to the 9th floor to ensure that only properly authorized individuals have access.

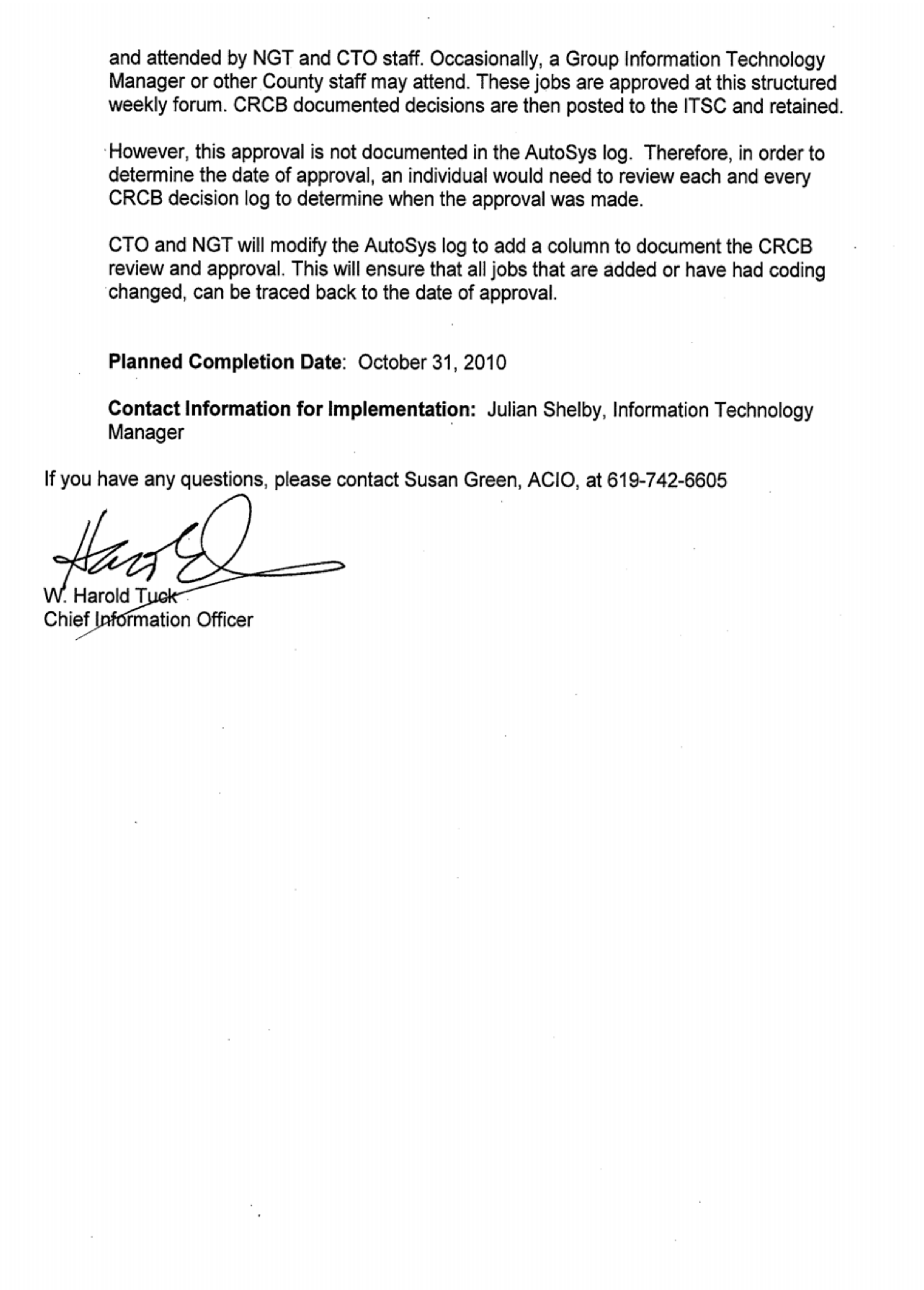
Planned Completion Date: October 31, 2010

Contact Information for Implementation: Julian Shelby, Information Technology Manager

Finding III: Job Scheduling Process Needs Improvement

OAAS Recommendation: The CTO and the NGT management should develop, update, review, approve, and implement the job scheduling procedures for all platforms processing County jobs. New or changed jobs should be properly approved and supporting documents should be retained in compliance with the County's records retention policies.

Action Plan: Since the inception of the Outsourcing Contract, all new jobs, or jobs with coding changes, to be scheduled and run in production are identified, reviewed, and discussed at the weekly CRCB (Change Release Control Board) meeting that is held



and attended by NGT and CTO staff. Occasionally, a Group Information Technology Manager or other County staff may attend. These jobs are approved at this structured weekly forum. CRCB documented decisions are then posted to the ITSC and retained.

However, this approval is not documented in the AutoSys log. Therefore, in order to determine the date of approval, an individual would need to review each and every CRCB decision log to determine when the approval was made.

CTO and NGT will modify the AutoSys log to add a column to document the CRCB review and approval. This will ensure that all jobs that are added or have had coding changed, can be traced back to the date of approval.

Planned Completion Date: October 31, 2010

Contact Information for Implementation: Julian Shelby, Information Technology Manager

If you have any questions, please contact Susan Green, ACIO, at 619-742-6605

W. Harold Tuck
Chief Information Officer