Internal Audit Department

ORANGE COUNTY
6th Largest County in the USA

Internal Control Audit:

AUDITOR-CONTROLLER'S AND TREASURER-TAX COLLECTOR'S $22 BILLION ELECTRONIC FUNDS TRANSFER PROCESSES

For the Period March 1, 2008
through March 31, 2010

Material Impact Audit

$22 BILLION ELECTRONIC FUND TRANSFERS PROCESSED ANNUALLY

We audited the Auditor-Controller's (A-C) and Treasurer-Tax Collector's (T-TC) Electronic Funds Transfer (EFT) processes. We evaluated manual and system controls designed to mitigate risks associated with EFT processing.

We found internal controls are adequate to provide reasonable assurance in all material regards for:

(1) Establishing, authorizing, and processing electronic funds transfers completely and accurately in the A-C and T-TC;
(2) Segregation of duties in the Quantum and Commercial Electronic Office systems, including application controls related to user access profiles, system enforced dual authorizations, and password settings; and
(3) Access and transmission of A-C and T-TC EFT payment files transmitted to Wells Fargo Bank.
(4) In addition, we found EFT processes are efficient and effective.

However, because of the materiality of EFT payments and the criticality of the absolute precision required to make these payments accurately, we identified **fifteen (15) Control Findings** related to improving compliance with existing procedures and enhancing existing controls for EFTs.

AUDIT NO: 2821
REPORT DATE: OCTOBER 14, 2010

Director: Dr. Peter Hughes, MBA, CPA
Deputy Director: Eli Littner, CPA, CIA
Senior Audit Manager: Michael Goodwin, CPA, CIA
Senior IT Audit Manager: Autumn McKinney, CPA, CIA, CISA
IT Audit Manager: Wilson Crider, CPA, CISA
Audit Manager: Lily Chin, CPA
Senior Internal Auditor: Lisette Free, CPA

RISK BASED AUDITING
GAO & IIA Peer Review Compliant – 2001, 2004, 2007, 2010

American Institute of Certified Public Accountants Award to Dr. Peter Hughes as 2010 Outstanding CPA of the Year for Local Government

2009 Association of Certified Fraud Examiners' Hubbard Award to Peter Hughes for the Most Outstanding Article of the Year

2008 Association of Local Government Auditors' Bronze Website Award

2005 Institute of Internal Auditors' Award for Recognition of Commitment to Professional Excellence, Quality, and Outreach

Independence • Objectivity • Integrity

ORANGE COUNTY BOARD OF SUPERVISORS' OC Internal Audit Department

GAO & IIA Peer Review Compliant - 2001, 2004, 2007, 2010

Providing Facts and Perspectives Countywide

RISK BASED AUDITING

Dr. Peter Hughes — **Ph.D., MBA, CPA, CCEP, CITP, CIA, CFE, CFF**
Director
Certified Compliance & Ethics Professional (CCEP)
Certified Information Technology Professional (CITP)
Certified Internal Auditor (CIA)
Certified Fraud Examiner (CFE)
Certified in Financial Forensics (CFF)
E-mail: peter.hughes@iad.ocgov.com

Eli Littner — **CPA, CIA, CFE, CFS, CISA**
Deputy Director
Certified Fraud Specialist (CFS)
Certified Information Systems Auditor (CISA)

Michael Goodwin — **CPA, CIA**
Senior Audit Manager

Alan Marcum — **MBA, CPA, CIA, CFE**
Senior Audit Manager

Autumn McKinney — **CPA, CIA, CISA, CGFM**
Senior Audit Manager
Certified Government Financial Manager (CGFM)

Hall of Finance & Records

12 Civic Center Plaza, Room 232
Santa Ana, CA 92701

Phone: (714) 834-5475 Fax: (714) 834-2880

To access and view audit reports or obtain additional information about the OC Internal Audit Department, visit our website: www.ocgov.com/audit

OC Fraud Hotline (714) 834-3608

Letter from Dr. Peter Hughes, CPA

Transmittal Letter

Audit No. 2821 **October 14, 2010**

TO: David Sundstrom, Auditor-Controller
Chriss Street, Treasurer-Tax Collector
Satish Ajmani, Chief Information Officer

FROM: Dr. Peter Hughes, CPA, Director
Internal Audit Department

SUBJECT: Internal Control Audit: Auditor-Controller's and Treasurer-Tax Collector's $22 Billion Electronic Funds Transfer Processes

We have completed an Internal Control Audit of the Auditor-Controller's and Treasurer-Tax Collector's Electronic Funds Transfer (EFT) Processes for the period March 1, 2008 through March 31, 2010, which included auditing transactions processed in the new CAPS+ financial system upgrade. The two offices processed over **$22 billion** in EFT transactions between March 2008 and March 2009. We performed this audit in accordance with our *FY 2008-09 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and the Board of Supervisors. Our final report is attached for your review.

Please note we have a structured and rigorous **Follow-Up Audit** process in response to recommendations and suggestions made by the Audit Oversight Committee (AOC) and the Board of Supervisors (BOS). As a matter of policy, our **first Follow-Up Audit** will begin at six months from the official release of the report. A copy of all our Follow-Up Audit reports is provided to the BOS as well as to all those individuals indicated on our standard routing distribution list.

The AOC and BOS expect that audit recommendations will typically be implemented within six months and often sooner for significant and higher risk issues. Our **second Follow-Up Audit** will begin at six months from the release of the first Follow-Up Audit report, by which time **all** audit recommendations are expected to be addressed and implemented.

At the request of the AOC, we are to bring to their attention any audit recommendations we find still not implemented or mitigated after the second Follow-Up Audit. The AOC requests that such open issues appear on the agenda at their next scheduled meeting for discussion.

We have attached three **Follow-Up Audit Report Forms**. Your department should complete the applicable form as our audit recommendations are implemented. When we perform our first Follow-Up Audit approximately six months from the date of this report, we will need to obtain the completed document to facilitate our review.

Each month I submit an **Audit Status Report** to the BOS where I detail any material and significant audit findings released in reports during the prior month and the implementation status of audit recommendations as disclosed by our Follow-Up Audits. Accordingly, the results of this audit will be included in a future status report to the BOS.

As always, the Internal Audit Department is available to partner with your staff so that they can successfully implement or mitigate difficult audit recommendations. Please feel free to call me should you wish to discuss any aspect of our audit report or recommendations.

Additionally, we will request your department complete a **Customer Survey** of Audit Services. You will receive the survey shortly after the distribution of our final report.

ATTACHMENTS

Other recipients of this report are listed on the **OC Internal Auditor's Report** on page 8.

Table of Contents (continued)

Internal Control Audit: Auditor-Controller's and Treasurer-Tax Collector's $22 Billion Electronic Funds Transfer Processes Audit No. 2821

For the Period March 1, 2008 through March 31, 2010

Table of Contents (continued)

OC Internal Auditor's Report

Audit No. 2821 **October 14, 2010**

TO: David Sundstrom, Auditor-Controller
Chriss Street, Treasurer-Tax Collector
Satish Ajmani, Chief Information Officer

FROM: Dr. Peter Hughes, CPA, Director
Internal Audit Department

SUBJECT: Internal Control Audit: Auditor-Controller's and Treasurer-Tax Collector's $22 Billion Electronic Funds Transfer Processes

Audit Highlight

We found that internal controls are adequate to provide reasonable assurance in all material regards over: (1) establishing, authorizing and processing electronic funds completely and accurately in the Auditor-Controller (A-C) and Treasurer-Tax Collector (T-TC); (2) segregation of duties in the Quantum and Commercial Electronic Office (CEO) systems, including application controls related to user access profiles, system enforced dual authorization, and password settings; and (3) access and transmission of A-C and T-TC EFT payment files transmitted to Wells Fargo Bank. In addition, EFT processes are efficient and effective.

We identified **fifteen (15) Control Findings** to improve compliance with existing procedures and enhance existing controls for EFTs.

OBJECTIVES

The Internal Audit Department conducted an Internal Control Audit of the Auditor-Controller's and Treasurer-Tax Collector's Electronic Funds Transfer (EFT) processes. Our audit included an evaluation of the adequacy and integrity of internal controls; testing compliance with department and County policies; and evaluating process efficiencies and effectiveness. Our audit was conducted in conformance with professional standards established by the Institute of Internal Auditors. The four objectives of our audit were to evaluate and test:

1. **Establishing, Authorizing and Processing EFTs:** We reviewed controls in the Auditor-Controller and Treasurer-Tax Collector for establishing and authorizing EFTs to ensure responsibilities for initiating, approving and releasing electronic funds are adequately segregated. Additionally, we reviewed controls to ensure EFTs are processed completely and accurately in accordance with County policy, departmental procedures and management's authorization.

2. **User Access and Application Controls:** For the Treasurer-Tax Collector's Quantum and Commercial Electronic Office (CEO) systems, we reviewed selected application controls to ensure adequate segregation of duties over EFTs including user access profiles, system enforced dual authorizations, and password settings.

3. **Access and Transmission Controls for EFT Payment Files:** We reviewed access and transmission controls in the Auditor-Controller, Treasurer-Tax Collector, and OC Enterprise Data Center (CEO/IT) for EFT files transmitted to Wells Fargo Bank (via the File Transfer Protocol server located at the OC Enterprise Data Center or directly by the T-TC) to ensure the EFT files are adequately protected.

4. **Efficiency/Effectiveness:** We determined if business processes are efficient and effective (no backlogs, duplication of work, or manual processes that could benefit from automation) as related to EFTs in the Auditor-Controller and Treasurer-Tax Collector.

RESULTS

We found that internal controls are adequate to provide reasonable assurance in all material regards for:

(1) Establishing, authorizing and processing electronic fund transfers completely and accurately in the Auditor-Controller and Treasurer-Tax Collector;
(2) Segregation of duties in the Quantum and Commercial Electronic Office systems, including application controls related to user access profiles, system enforced dual authorizations, and password settings; and
(3) Access and transmission of A-C and T-TC EFT payment files transmitted to Wells Fargo Bank processed via the FTP server located at the OC Enterprise Data Center (CEO/IT).
(4) In addition, we found that EFT processes are efficient and effective.

However, because of the materiality of EFT payments and the criticality of the absolute precision required to make these payments accurately, we identified **fifteen (15) Control Findings** related to improving compliance with existing procedures and enhancing existing controls for EFTs. See further discussion in the *Detailed Findings, Recommendations and Management Responses* section of this report. See *Attachment A* for a description of Report Item Classifications. Our audit disclosed:

- **Objective #1 – Establishing, Authorizing and Processing Electronic Fund Transfers (EFTs):** We *reviewed controls in the Auditor-Controller and Treasurer-Tax Collector for establishing and authorizing EFTs to ensure responsibilities for initiating, approving and releasing electronic funds are adequately segregated. Additionally, we reviewed controls to ensure EFTs are processed completely and accurately in accordance with County policy, departmental procedures and management's authorization.*

- **Results:** We found responsibilities for establishing, authorizing and processing electronic funds are adequately segregated in the Auditor-Controller and Treasurer-Tax Collector to provide reasonable assurance that EFTs are processed completely and accurately in accordance with County policy, departmental procedures and management's authorization in all material regards. We noted **six (6) Control Findings** in the areas of authorized signatures, data entry, authorization of EFTs, release of payments, and ensuring correct bank account numbers. (See Findings 1 through 6 below)

- **Objective #2 – User Access and Application Controls:** *For the Treasurer-Tax-Collector's Quantum and Commercial Electronic Office (CEO) systems, we reviewed selected application controls to ensure adequate segregation of duties including: user access profiles, system enforced dual authorizations, and password settings.*

- **Results:** We found selected application controls are adequate in the Treasurer-Tax Collector's Quantum and CEO systems and provide reasonable assurance for segregation of duties including user access profiles, system enforced dual authorizations, and password settings in all material regards. We noted **two (2) Control Findings** concerning access to the CEO system and Quantum account and password settings. (See Findings 7 and 8 below)

- **Objective #3 – Access and Transmission Controls for EFT Payment Files:** We *reviewed controls over access and transmission of the EFT payment files transmitted to Wells Fargo Bank to ensure the files are adequately protected. The files reside at the Treasurer-Tax Collector server, the Auditor-Controller/CAPS+ File Transfer Protocol (FTP) server, and the OC Enterprise Data Center FTP server (CEO/IT).*

- **Results:** We found controls are adequate over access and transmission of the EFT payment files at the Treasurer-Tax Collector, Auditor-Controller/CAPS+, and OC Enterprise Data Center (CEO/IT) to provide reasonable assurance that the files are protected. We noted **six (6) Control Findings** in the areas of CAPS+ server accounts, FTP administrative accounts, and firewall configuration. (See Findings 9 through 14 below)

- **Objective #4 – Efficiency/Effectiveness:** We determined if b*usiness processes are efficient and effective (no backlogs, duplication of work, or manual processes that could benefit from automation) as related to EFTs in the Auditor-Controller and Treasurer-Tax Collector.*

- **Results:** We found overall processes are efficient and effective concerning the Auditor-Controller and Treasurer-Tax Collector's EFT processes. However, we noted **one (1) Control Finding** concerning Quality Assurance reviews performed in A-C Claims & Disbursing to ensure effectiveness in processing EFTs. (See Finding 15 below)

BACKGROUND

The Auditor-Controller (A-C) and Treasurer-Tax Collector (T-TC) processed approximately **$22 billion** in Electronic Fund Transfers (EFTs) between March 2008 and March 2009. EFTs consist of wire transfers and Automated Clearing House (ACH) transactions. These transactions are processed either by the (1) Treasurer-Tax Collector, (2) Auditor-Controller, or (3) Other County departments/agencies. A brief description of each follows:

1. **Treasurer-Tax Collector** processes EFTs using the Quantum and Commercial Electronic Office systems. For the one year period between March 2008 and March 2009, the T-TC processed approximately **$20 billion** in EFTs as follows:

   - **Disbursements Requested by County Departments ($1.5 billion):** A manual *EFT/On Demand Wire Form* is used by departments/agencies to request electronic payments. The form and supporting documents are sent to the A-C for disbursement review/approval and to record the transactions in the General Ledger (CAPS+). A copy of the form is emailed to the T-TC to process the EFT. Upon receiving approval from the A-C, the T-TC approves and releases the EFT. These EFTs payments are made by either:

     - **Automated Clearing House ($733 million)** payments are electronic payments made a day after the scheduled payment date. Examples include accounts payable for vendor and trust payments.

- **Wire Transfers ($779 million)** are electronic payments made the same day as the scheduled payment date. Wire transfers are used for accounts payable for debt service and trust payments.

- **Treasurer Investments ($13.4 billion)** relates to investment activities performed by the T-TC on behalf of the County, Teeter funds, and Department of Education.

- **Intra-bank Transfers Out ($400 million)** are transfers between the various bank accounts managed by the T-TC including Teeter and Department of Education.

- **Department of Education ($4.4 billion)** payments are made to schools to fund operations (payroll and other school related expenses).

- **Payroll, Sales, and Landfill Tax Payments ($229 million)** are payments for Federal and State payroll taxes, State Board of Equalization payments, Internal Revenue Service payments, and landfill taxes. These payments are processed using the Commercial Electronic Office system.

The T-TC generates an EFT file from the Quantum system. This EFT file is subsequently formatted and transmitted directly to Wells Fargo Bank using an in-house developed Wire Transfer Application. The Wire Transfer Application uses Valicert which is a file transmission software recommended by Wells Fargo Bank that utilizes encryption during transmission.

In addition, as a back-up to Quantum and for payroll taxes, sales taxes, and landfill taxes, the T-TC enters EFT data directly into the Commercial Electronic Office (CEO) system. The CEO system is hosted by Wells Fargo Bank and provides a direct interface to the bank's EFT operations.

2. **Auditor-Controller** processes EFTs using CAPS (replaced by CAPS+ on July 1, 2009). For the one year period between March 2008 and March 2009, the A-C processed approximately **$2 billion** EFTs in CAPS:

   - **CAPS+ EFTs (previously named PVEs) ($2 billion)** are Automated Clearing House (ACH) payments made via the CAPS+ system. Prior to CAPS+, these electronic payments were named Payment Voucher Electronic (PVEs). CAPS+ EFTs are mainly used for e-commerce (e.g. Office Depot), trust fund payments, revolving fund replenishments, purchasing card payments, and property tax apportionments. The CAPS+ EFTs are entered and processed in CAPS+ by the A-C/Claims and Disbursing Unit or via system interfaces from other County departmental systems.

   - **Treasurer-Tax Collector EFTs Recorded in CAPS+:** As CAPS+ is the County's system of record for financial transactions, the A-C also approved and recorded in CAPS+ the **$1.5 billion** in disbursements requested by County departments and processed as EFTs by the T-TC. See "**Disbursements Requested by County Departments"** above on page 3.

CAPS+ creates EFT files which are transmitted from the CAPS+ File Transfer Protocol (FTP) server to the OC Enterprise Data Center's FTP server via Valicert. Valicert is the file transmission software recommended by Wells Fargo Bank that utilizes encryption during transmission. The CAPS+ EFT files are then sent to Wells Fargo Bank for processing also using Valicert. The process includes confirmation files from Wells Fargo Bank acknowledging receipt of the files. This method is also used by the Social Services Agency and Child Support Services for their EFT payments (see below).

3. **Other Department/Agency EFT Payments.** Certain departments/agencies (Social Services Agency, Child Support Services, Health Care Agency, and OC Community Resources) do not use the T-TC or A-C to process certain EFTs. Instead, these departments process their own EFT payments in a subsidiary system using one of the three methods listed below. Examples of these EFT payments include: CalWIN cash assistance payments and electronic benefit transfers (EBTs), child support payments, healthcare provider payments, and Section 8 housing assistance payments.

   As described in the Scope Section below, these transactions were excluded from our scope, except for our review of EFT file security if the department (such as SSA and CSS) uses the File Transfer Protocol (FTP) server located at the OC Enterprise Data Center (CEO/IT).

   - **FTP Server (OC Enterprise Data Center - CEO/IT)** is used by departments to transmit payment files to the bank. The department/agency system creates a payment file which is transmitted to the FTP server at the OC Enterprise Data Center. The payment file is then transmitted to Wells Fargo Bank for processing. The process includes confirmation files from Wells Fargo Bank acknowledging receipt of the files. The department/agency also communicates (e-mail or system interfaces) with the A-C to record the transactions in the General Ledger (CAPS+). The Social Services Agency and Child Support Services use this method.

   - **FTP Server (Department/Agency)** is similar in concept to the process for the FTP Server located at the OC Enterprise Data Center (CEO/IT) except the department sends the files utilizing an in-house FTP server (i.e. not located at the OC Enterprise Data Center). Also, the Valicert file transmission software may not be used. The department communicates with the A-C to record the transactions in the General Ledger (CAPS+). OC Community Resources uses this method for Section 8 housing assistance payments.

   - **Zero-Balance Accounts (ZBAs)** are bank accounts in which a balance of zero is maintained by automatically transferring funds from a master account in an amount only large enough to cover payments presented. The department/agency subsidiary systems interface with CAPS+ to record the transactions in the General Ledger. The Health Care Agency and Social Services Agency use this method.

Information Technology Systems
The following systems support the Auditor-Controller's and Treasurer-Tax Collector's EFT processes:

- **AdvantGard (Quantum):** A third-party developed application used by the T-TC to process electronic payments (ACH and wire transfers). Quantum generates a payment file that is subsequently formatted and transmitted to Wells Fargo Bank using the below Wire Transfer Application.

- **Wire Transfer Application:** An in-house developed system that prepares/formats the Quantum payment file for transmission to Wells Fargo Bank. The Wire Transfer Application uses Valicert which is a file transmission software recommended by Wells Fargo Bank that utilizes encryption during transmission.

- **Commercial Electronic Office (CEO):** A third-party developed application hosted by Wells Fargo Bank and used by T-TC to submit ACH and wire transfer payments. The T-TC uses the CEO ACH module to process specific types of electronic payments such as payroll taxes, sales tax, and landfill taxes. CEO is also the backup system for Quantum to perform EFTs. The CEO system provides a direct interface to the bank's EFT operations.

- **Countywide Accounting and Personnel System (CAPS+):** A third-party developed application providing Accounting, Procurement, Budget, and Financial Reporting functionality. CAPS+ is the system of record for County financial transactions. The County upgraded to the CAPS+ financial system effective July 1, 2009. CAPS+ generates payment files that are transmitted (via a FTP server located at the OC Enterprise Data Center – CEO/IT) and forwarded to Wells Fargo Bank for processing.

SCOPE

Our audit evaluated internal controls and processes over Electronic Funds Transfers (EFTs) for the period from March 1, 2008 through March 31, 2010 in the Auditor-Controller and Treasurer-Tax Collector. Our scope included the following elements:

- We identified the amount of EFTs processed by the A-C and T-TC, and documented related processes and controls (manual and automated) over establishing, entering, approving, releasing, and reconciling electronic payments by performing interviews, observations, and process walk-throughs.

- We determined if controls were in place to safeguard EFTs, and to detect and prevent an employee or vendor from misdirecting funds.

- We audited the T-TC's Quantum and Commercial Electronic Office systems for selected application controls relating to segregation of duties including user access profiles, system enforced dual authorizations, and system password settings.

- Our audit covered selected controls for both CAPS and CAPS+. As such, we performed additional work to document and/or test the changes to selected processes and controls based on the CAPS+ implementation effective July 1, 2009.

- We reviewed access and transmission controls for the EFT files to Wells Fargo Bank to ensure EFT files are adequately protected. The files reside at the T-TC server, the A-C/CAPS+ FTP server, and the OC Enterprise Data Center FTP server (CEO/IT).
- We evaluated the efficiency and effectiveness of processes under audit for backlogs, duplication of work, or manual processes that would benefit from automation.

SCOPE EXCLUSIONS

Our audit scope **did not** cover the following areas:

- Auditor-Controller Satellite Units: We obtained an understanding of processes and controls in selected A-C Satellite Units to determine how EFTs are initiated and authorized; however, we did not audit processes and controls in the Satellite Units.
- CAPS+ Application Controls: We did not perform a comprehensive review of application controls for the new CAPS+ system such as for the vendor table and accounts payable processing. We previously provided informal internal controls feedback during the CAPS+ implementation project before the go-live date of July 1, 2009. Also in our prior audit (No. 2720-4), we audited controls over the pre-CAPS+ vendor invoice processing and vendor table administration. Additionally, we have started a separate audit of CAPS+ user access/segregation of duties (No. 2947).
- General Information Technology Controls: We did not review general IT controls for the systems under audit. The general controls for the Quantum and CEO systems were reviewed previously by the Auditor-Controller's Internal Audit Unit during their annual Treasury Funds Audit.
- Other County Department/Agency EFT Payments: We obtained a high-level understanding of controls in selected departments/agencies where EFTs are initiated and processed directly with the banks and are not processed by the A-C or T-TC. However, we did not perform any testing of these controls, including approvals and reconciliations, with the exception of our review of EFT file security if the department's file transmission uses the FTP server located at the OC Enterprise Data Center.

Management's Responsibilities for Internal Controls

In accordance with the Auditor-Controller's County Accounting Manual section S-2 *Internal Control Systems*, "All County departments/agencies shall maintain effective internal control systems as an integral part of their management practices. This is because management has primary responsibility for establishing and maintaining the internal control system. All levels of management must be involved in assessing and strengthening internal controls. Control systems shall be continuously evaluated and weaknesses, when detected, must be promptly corrected." The criteria for evaluating an entity's internal control structure is the Committee of Sponsoring Organizations (COSO) control framework. Our Internal Control Audit enhances and complements, but does not substitute for the Auditor-Controller's, Treasurer-Tax Collector's, and CEO/Information Technology's continuing emphasis on control activities and self-assessment of control risks.

Inherent Limitations in Any System of Internal Control

Because of inherent limitations in any system of internal controls, errors or irregularities may nevertheless occur and not be detected. Specific examples of limitations include, but are not limited to, resource constraints, unintentional errors, management override, circumvention by collusion, and poor judgment. Also, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or the degree of compliance with the procedures may deteriorate. Accordingly, our audit would not necessarily disclose all weaknesses in the Auditor-Controller's, Treasurer-Tax Collector's, and CEO/Information Technology's operating procedures, accounting practices, and compliance with County policy.

Acknowledgment

We appreciate the courtesy extended to us by the Auditor-Controller, Treasurer-Tax Collector, and CEO/Information Technology during our audit. We also appreciate the assistance of other various County departments/agencies we contacted as part of this audit. If we can be of further assistance, please contact me directly; or Eli Littner, Deputy Director at 834-5899; or Michael Goodwin, Senior Audit Manager at 834-6066; or Autumn McKinney, Senior IT Audit Manager, at 834-6106.

Attachments

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Thomas G. Mauk, County Executive Officer
Bob Franz, Deputy CEO, Chief Financial Officer
Shaun Skelly, Chief Deputy, Auditor-Controller
Jan Grimes, Director, Central Accounting Operations, Auditor-Controller
Bill Castro, Director, Satellite Accounting Operations, Auditor-Controller
Victoria Ross, Senior Manager, Claims and Disbursing, Auditor-Controller
Salvador Lopez, Claims Manager, Claims & Disbursing, Auditor-Controller
Phil Daigneau, Director, Information Technology, Auditor-Controller
Paul Gorman, Chief Assistant Treasurer-Tax Collector
Jennifer Burkhart, Assistant Treasurer-Tax Collector
Kim Hansen, Cash Manager, Treasurer-Tax Collector
Joel Manfredo, Chief Technology Officer, CEO/Information Technology
KC Roestenberg, Director, CEO/IT - Enterprise IT Shared Services
Mark Khanlar, Manager, CEO/IT - Enterprise IT Shared Services/Network Platform Services
Foreperson, Grand Jury
Darlene J. Bloom, Clerk of the Board of Supervisors

Audit Objective #1 – Establishing, Authorizing and Processing EFTs

Our objective was to review controls in the Auditor-Controller and Treasurer-Tax Collector for establishing and authorizing EFTs to ensure responsibilities for initiating, approving and releasing electronic funds are adequately segregated. Additionally, we reviewed controls to ensure EFTs are processed completely and accurately in accordance with County policy, departmental procedures and management's authorization. Strong internal and information technology controls in these areas are vital to prevent unauthorized EFTs from occurring. Appropriate segregation of duties provides assurance that one individual cannot control all aspects of an EFT without oversight and approval by others.

We tested on a sample basis **forty-two (42) EFTs** totaling approximately **$105 million** to determine if they were properly established and authorized; supervisory reviews were performed and documented; appropriate supporting documentation was maintained; approvals were made by "authorized" individuals in departments/agencies and Auditor-Controller; and funds were released to the proper account. Our sample included CAPS/CAPS+ Payment Voucher Electronic/EFT payments; Quantum wire transfer/ACH payments; Commercial Electronic Office payments; and CAPS+ miscellaneous vendor EFT payments.

Process and Control Strengths

Our audit found responsibilities for initiating, approving and releasing EFTs are adequately segregated in the Auditor-Controller and Treasurer-Tax Collector, and EFTs are processed completely and accurately in accordance with County policy, departmental procedures and management's authorization. Process and control strengths noted during the audit include:

Auditor-Controller:

A-C Controls for CAPS+ Processed EFTs:

- ✓ CAPS/CAPS+ EFTs can only be made to an established vendor (i.e. must be set-up on the vendor table).
- ✓ For CAPS/CAPS+ EFTs, a standardized, manual *EFT Authorization* is used by all departments/agencies to request that a vendor be established in CAPS/CAPS+.
- ✓ Pre-note tests validate vendor bank account information data on *EFT Authorization Forms.*
- ✓ The CAPS+ vendor table is now the responsibility of the A-C's General Ledger Unit, which was formerly performed by the A-C Claims & Disbursing - Compliance Unit. Set-up and/or modification of vendor and EFT bank information is restricted to authorized users. To add or change vendor information, CAPS+ has a system enforced rule requiring a person other than the transaction creator to approve the transaction. An additional supervisory review of bank account information is also required for CAPS+/EFT vendors.
- ✓ A-C Claims & Disbursing has a *Payment Voucher Approval Policy* that describes a manual control of requiring supervisory/management approval based on dollar thresholds of the payments (see Finding No. 4 below for review thresholds).

- ✓ CAPS+ EFT information is input into CAPS+ by Payment Auditors in A-C Claims & Disbursing or Satellite Accounting. CAPS+ automatically infers vendor name and bank information against the vendor table.

- ✓ For CAPS, A-C generated and reviewed PVE daily exception reports. In CAPS+, the exceptions (errors) are corrected during data entry validations. The A-C also performs daily and monthly EFT reconciliations between T-TC records and the General Ledger to ensure reconciling items are manually investigated and resolved timely.

A-C Controls for EFTs Processed by Treasurer-Tax Collector:

- ✓ A manual *Electronic Fund Transfer* (CAPS)/*On Demand Wire* (CAPS+) Form is used by departments/agencies to request EFT payments for accounts payable and trust payments.

- ✓ The manual *EFT/On Demand Wire Forms* are submitted to A-C Claims & Disbursing or A-C Satellite Accounting Units. The Payment Auditors record the EFTs in CAPS+.

- ✓ Additionally, the Payment Auditors review for legal authority to pay by verifying the *EFT/On Demand Wire Forms* from departments/agencies are properly prepared, accurate, valid, supported, and authorized prior to initiation of an electronic payment, except in departments/agencies with A-C Satellite Accounting Units where the reviews and approvals are completed on behalf of A-C Claims & Disbursing. The Payment Auditors sign and approve the forms.

- ✓ A-C Check Writing reviews *EFT/On Demand Wire Forms* for approval signatures by Claims & Disbursing before submitting as final and forwarding them to the T-TC.

Treasurer-Tax Collector:

- ✓ The T-TC receives electronic versions by email of the *EFT/On Demand Wire Forms* from the originating department/agency. An Accounting Technician enters the information into Quantum and waits for the approved and signed form from A-C Check Writing.

- ✓ The T-TC verifies the bank and address (account numbers) by ensuring the *EFT/On Demand Wire Form* bank information agrees with Quantum bank information, and ensures the A-C approvals are documented in the *EFT/On Demand Wire Form*. Once this information is verified, it is forwarded for review and approval.

- ✓ Any changes to a vendor (counterparty) in Quantum requires supervisory review and approval.

- ✓ EFT transactions are confirmed by Wells Fargo Bank to the T-TC, who then notifies the originating departments that the electronic funds were transferred.

- ✓ For Commercial Electronic Office EFTs, all transactions are documented on a manual log and initialed by the initiator, approver, and releaser. Because the approver is also the releaser in CEO, the manual log is kept to document separate persons for "approving" and "releasing" EFTs.

(See Audit Objective #2 – User Access and Application Controls below for IT controls and strengths related to the Quantum and CEO systems.)

The following are areas where processes and controls should be enhanced:

Finding No. 1 – Approval Signatures Not on Authorized List (Control Finding)

We noted **two (2) of forty-two (42) EFTs** selected for testing (**$2.1M and $118,000**) were processed with an agency's personnel signature that is not on the agency's *Authorized Signature Form or Access Request Form.* This resulted in payments that were not properly approved by an authorized agency personnel. This occurred in an A-C Satellite Unit where the EFT payments were reviewed and authorized for payment.

Approval of a transaction is an important control activity; therefore, only authorized agency personnel may approve payment transactions. Departments/agencies are responsible for providing and updating all authorized signatures on the Orange County Auditor-Controller *Authorized Signature Form or Access Request Form*, effective 7/1/09. *County of Orange Accounting Manual, M-1, Authorized Signature List,* requires each County agency to maintain an updated list of authorized signatures for the purpose of verifying agency employee signatures placed on various documents sent to the Auditor-Controller.

Recommendation No. 1
Auditor-Controller ensure its Satellite Accounting Units verify the payment approval with the corresponding agency's authorized signature forms/access request forms prior to processing EFT payments.

Auditor-Controller Management Response:
Concur. Satellite Accounting Units will be reminded when processing EFT payments to always check the validity of the agency's authorized signer to the CAPS+ Access Request form and to only process EFT requests signed by an authorized signer. Additionally, written procedures are estimated to be completed by March 31, 2011.

Finding No. 2 – Missing Authorized Signatures on EFT/On Demand Wire Forms (Control Finding)

We noted **one (1) of forty-two (42) EFTs** selected for testing (**$353**) did not have the agency's authorized signature on the *EFT/On Demand Wire Form*.

Designated department personnel reviewed and approved the General Accounting Trust (GAT) document in CAPS+ and electronically workflowed it to A-C Check Writing Unit along with the hard copy *EFT/On Demand Wire Form*. However, the *EFT/On Demand Wire Form* was missing the authorized department's signature. Without an authorized signature on the form, there is increased risk that unauthorized transactions could occur.

Recommendation No. 2
Auditor-Controller Check Writing ensure that hard copy *EFT/On Demand Wire Forms* contain authorized signatures before releasing payments.

Auditor-Controller Management Response:

Concur. Check Writing will be reminded to review for authorized signature prior to submitting the document to CAPS+. Additionally, written procedures are estimated to be completed by December 30, 2010.

Finding No. 3 – Data Entry Errors Not Detected (Control Finding)

We noted **two (2) of forty-two (42) EFTs** selected for testing were processed with data entry errors that were not detected in A-C Claims & Disbursing's payment reviews:

- One miscellaneous vendor payment of **$69,581** to BenefitsCorp contained incorrect General Ledger account coding. This transaction is a recurring payment initiated and authorized in Claims & Disbursing. We tested two other transactions to BenefitsCorp and found they had the correct account coding.

- For one "miscellaneous trust" vendor payment to the Internal Revenue Service for **$353,** the vendor name and address was indicated in CAPS+ only as "." For "miscellaneous vendor" payments, CAPS+ does not automatically infer the vendor name and address from the vendor table for miscellaneous vendors. Miscellaneous vendors are intended to be for one-time payments, and every document should have a payee/vendor name.

A-C Claims & Disbursing's review did not detect the above data entry errors. Strong internal controls require verification of transactions after they have been entered into the system to detect if erroneous documents are processed for payment. In addition, there is a risk of loss when transactions are not completely and accurately recorded.

Recommendation No. 3

Auditor-Controller Claims & Disbursing ensure payment processors adequately review the data entered against supporting documentation, including vendor addresses, to ensure it is accurate and complete prior to processing payments.

Auditor-Controller Management Response:

Partially concur. Payment processors do review supporting documentation to ensure accuracy, but they do not audit account coding. It is the responsibility of the submitting department to ensure that account coding is correct. Additionally, we agree that all "miscellaneous trust" vendor payments must have a payee/vendor name. Check Writing will be reminded to review the input of the vendors name prior to submitting the GA Trust Fund Payment document. Additionally, written procedures are estimated to be completed by December 30, 2010.

Findings Nos. 4 and 5 – Payment Authorization Procedures Not Standardized (Control Finding)

Procedures for reviewing and authorizing payments in the A-C Satellite Accounting Units are not consistent with the procedures used in the A-C Claims & Disbursing Unit for reviewing and authorizing payment requests for other department/agencies.

The A-C has out-stationed **Satellite Accounting** Units in certain departments/agencies (CEO/Public Finance, Health Care Agency, Social Services Agency, OC Waste & Recycling, OC Community Resources, John Wayne Airport, and OC Public Works), whose responsibilities include reviewing and authorizing payment requests on behalf of the A-C. We noted that these departments/agencies each have different manual payment review and authorization procedures involving signature authority and dollar thresholds. A manager in the Satellite Unit signs and authorizes payment requests and forwards them to A-C Claims & Disbursing for payment. Because requirements in departments vary, A-C Claims & Disbursing relies solely on the Satellite Unit manager's authorized signature for approving the payment request, and the below supervisory approval thresholds used in A-C Claims do not apply to the Satellite Units.

In the departments/agencies that do not have Satellite Accounting Units, A-C Claims & Disbursing has responsibility for reviewing and authorizing payment requests. A-C Claims' Payment Auditors review and audit each department payment request. For payment request amounts that exceed the following thresholds, additional manual supervisory/management review is required before approving the payments:

Below $100,000	***No supervisory review/approval required (All payments under $100K are reviewed by Payment Auditors, but without supervisory reviews)***
$100,000 to $499,999	***Requires a Unit Supervisor review/approval***
$500,000 to $999,999	***Requires a Unit Supervisor & Claims Unit Manager review/approval***
At or Over $1,000,000	***Requires a Unit Supervisor & Claims Unit Manager & Claims/Disbursing Senior Manager review/approval***

Our testing of payment authorizations in **A-C Claims & Disbursing** disclosed:

- The A-C Claims & Disbursing Senior Manager signed as reviewer/approver for two dollar-limit thresholds (e.g. $100,000 and $500,000) on the same EFT payment. The intent of this control is to have two different individuals approve payments based on higher dollar amounts.

- For payments over $1,000,000, we noted instances where only the A-C Claims & Disbursing Senior Manager reviewed and signed the payment request, with no reviews performed by a Unit Supervisor or the Claims & Disbursing Unit Manager.

- There are no supporting documents or detailed reviews by the A-C Claims & Disbursing staff of EFTs from departments/agencies that are processed as "interfaces." The above review thresholds do not apply to the payment requests via interfaces.

- No supporting documents accompany the *EFT/On Demand Wire Forms* and the A-C Claims & Disbursing staff relies solely on department's authorized signer to approve payments.

Our testing of payment authorizations in **A-C Satellite Accounting Units** disclosed:

- There are no standardized procedures or basic requirements for the Satellite Accounting Units concerning A-C responsibilities for approving payment requests.

- Some Satellite Accounting Units authorized signers documented their review in the A-C Claims & Disbursing section of the payment request; while others signed the forms in the section stating "Expenditures Authorized and Approved By."

- The A-C Claims & Disbursing Manager signed as "approver" on Satellite Accounting payment request forms; however, this approval was based solely on the existence of an authorized A-C Satellite Accounting Unit signature from the requesting department. Thresholds requiring additional supervisory reviews and approval are not used by Claims & Disbursing when approving Satellite Unit payments.

- With the implementation of CAPS+, the two main policies and procedures for processing payments are Procedure 2101, *Processing General Accounting Trust Payments (GAT) and On Demand Wire Trust Payments (MDW)*, and Procedure 2102, *Payments and Refunds.* Although the procedures instruct individuals to create, review and approve payments accurately, the policy is silent on the required steps for reviewing and approving payments.

Payment Requests Under $100,000

Payment requests under $100,000 are reviewed by A-C Payment Auditors; however, they do not receive a supervisory review in A-C Claims or in certain A-C Satellite Accounting Units. Although it is possible for Payment Auditors to initiate and process an unauthorized vendor payment, this would require collusion between the two parties (Payment Auditor and vendor). However, there still must be funds in the account, and any unauthorized payment may or may not be detected depending on the materiality by the department charged for the payment.

In addition, a memo from the Auditor-Controller was issued on April 5, 2010 stating that the "central accounts payable staff will reduce the level of effort on reviewing certain payments below $5,000 per invoice." There appears to be a trend to place more reliance on department/agency approvals. See Finding No. 15 under **Audit Objective #4 – Efficiency and Effectiveness** concerning this issue.

Based on payment data from CAPS+, between July 1, 2009 and March 31, 2010:

- Payments Less Than $100,000: There were 316,532 transactions processed totaling $520 million. About 9%, or $48 million, were entered into CAPS+ via interface files from departments/agencies subsidiary systems.

- Payments Greater Than $100,000: There were 3,124 transactions totaling $3.2 billion. About 38%, or $1.2 billion, were entered into CAPS+ via interface files from departments/agencies subsidiary systems.

Department Interfaces

Some department interface payments (e.g., OC Public Works telephone services and utilities; and A-C Tax Unit tax apportionments) are reviewed by A-C staff prior to payment; however, we noted **there is no review performed in A-C Claims & Disbursing of the department interface payment transactions (even if more than $100,000)** other than to reconcile the interface file record counts and ensure an authorized departmental signature was received for the interface file as a whole.

Recommendation No. 4

Auditor-Controller should evaluate if standardized policies and procedures for authorizing and approving disbursements can be established to ensure they are consistently applied both in A-C Claims & Disbursing and the A-C Satellite Accounting Units. The standardized procedures should include scope of the reviews and specific review criteria that can be incorporated into department/agency policy and procedures.

Auditor-Controller Management Response:

Concur. Auditor-Controller will be developing uniform guidelines and criteria for reviewers to follow and anticipated completion date is March 31, 2011.

Recommendation No. 5

Auditor-Controller should also evaluate whether disbursements processed as department interfaces should be subject to Auditor-Controller review and approval thresholds described above, and if support documentation should be required as part of the review process.

Auditor-Controller Management Response:

Concur. Department interfaces will be evaluated as part of reviewing the scope of Quality Assurance testing which is part of Recommendation No. 15 and is estimated to be completed by March 31, 2011.

Finding No. 6 – Errors and Omissions of Bank Account Numbers (Control Finding)

We noted **six (6) of forty-two (42) EFTs** tested were released to account numbers that differ from the banking information as stated on the *Electronic Funds Transfer Form/On Demand Wire Forms.* Specifically, the following was noted:

1. Two (2) payments (**$1,600,000 and $2,000,000**) listed transposed bank account numbers on the *On Demand Wire Form* based on the account number shown on the department's wire transfer instructions. We were informed the bank accepted the wires and the vendor was paid despite the incorrect account numbers on the *On Demand Wire Form.*

2. Four (4) *EFT/On Demand Wire Forms* for federal and state tax deposits payments totaling over **$22 million** did not include the recipients' ABA bank account numbers.

With such errors and omissions, there is an increased risk of liability and/or loss of funds since the County may not become aware for some time of payments not received (usually when the intended recipient notifies the payment was not received). In addition, non-repetitive electronic fund payments have a higher risk of loss resulting from improperly coded account numbers.

Recommendation No. 6

Auditor-Controller Claims & Disbursing Unit and Satellite Accounting offices ensure during their review that bank account codes and ABA numbers are correctly documented prior to approving EFTs.

Auditor-Controller Management Response:

Concur. Auditor-Controller Claims will remind Central Operations and Satellite Accounting Offices to review and ensure accuracy of these numbers. Additionally, written procedures are estimated to be completed by March 31, 2011.

Audit Objective #2 – User Access and Application Controls

Our objective was to review selected application controls in the Treasurer-Tax Collector's Quantum and Commercial Electronic Office (CEO) systems to ensure adequate segregation of duties over EFTs including user access profiles, system enforced dual authorizations, and password settings.

User Access and Application Control Strengths

Our audit found that controls are in place in the Treasurer-Tax Collector's Quantum and CEO systems to ensure an adequate segregation of duties over EFTs including user access profiles, system enforced dual authorizations, and password settings. Process and control strengths noted include:

Quantum Application Controls:

- ✓ System controls prevent users from creating, approving and releasing their own transactions (user roles are adequately segregated).

- ✓ System enforced dual authorization (i.e. requires two different users) for the following:
  - To enter, approve, release EFTs (one extra user for total of three unique users).
  - To set-up/modify counterparty (recipient of funds) info (i.e. bank account number).
  - To assign user rights/groups (both Systems Administrator and Security Approver).
  - To change system default settings such as password settings and dual authorization settings (both Systems Administrator and Security Approver).

- ✓ When entering an EFT transaction, the counterparty information is automatically inferred by the counterparty set-up (functions similar to a vendor table). Approved counterparty must be set-up first before entering an EFT.

- ✓ Any changes to a vendor already established in Quantum must be approved.

- ✓ Approver cannot modify the EFT such as bank account or amount (i.e. can only approve or reject the wire).

- ✓ Releaser cannot modify the EFT such as bank account or amount (i.e. can only release or reject the wire).

- ✓ System provides account and password management functions.

CEO Application Controls:

- ✓ Wells Fargo Bank hosts the application and there is limited ability for the T-TC to change application controls and security/password settings. Self-administration features are limited.

- ✓ System controls prevent users from creating and approving their own transactions (user roles are adequately segregated).

- ✓ System enforced dual authorization (i.e. requires two different users) for the following:
  - To enter and approve/release EFTs.
  - To assign user rights/products (only Company Administrators and Group Administrators within their group).
  - To reset passwords (only Company Administrators and Group Administrators within their group).
  - To set-up/modify EFT settings/preferences such as transaction limits, currency type, authorizations (only Company Administrators).
  - To maintain tokens such as assign tokens to users (only Company Administrators).
  - To change the dual authorization settings (only Company Administrators).

- ✓ Approver/Releaser cannot modify the EFT such as bank account or amount (i.e. can only accept or reject the EFT).

- ✓ RSA SecurID token is needed to access high risk activities such as dual authorization settings and processing EFTs.

- ✓ Passwords must be six to eight characters in length and consist of letters and/or numbers (no special characters are required; however risk is mitigated since there are additional token controls above).

- ✓ The system deactivates a user automatically if there is no log-on activity for 60 days.

(See **Audit Objective #1 – Establishing, Authorizing and Processing EFTs** above for manual controls and strengths.)

The following is where controls could be improved for user access and application controls:

Finding No. 7 – Remove CEO System EFT "Release" Role for EFT Manual Approvers (Control Finding)

Commercial Electronic Office (CEO) system controls prevent users from creating and releasing (approving/release) their own transactions. The T-TC has also implemented a manual approval of the EFT after it has been created and before it has been released in CEO.

Two individuals in the T-TC who are manual approvers of EFTs were also given the ability to "release" EFTs in the CEO system. The system "release" access was granted as an emergency back-up. Good internal controls require proper segregation of these duties. As there appears to be a sufficient number of users with "release" authority, the "release" access granted to the two manual approvers should be removed.

Recommendation No. 7
Treasurer-Tax Collector should remove the "release" access within the CEO system for the two manual approvers of EFTs.

Treasurer-Tax Collector Management Response:
Concur. This recommendation has been implemented.

Finding No. 8 – More Restrictive Quantum Account and Password Settings (Control Finding)

The Quantum application security was configured to allow a user to log-on multiple times, the password filters did not provide for any password complexity, and password uniqueness was set to "one" password. These settings provide for easier user administration. However, these settings do not conform with best practices. These settings increase the probability that an account may be used inappropriately by allowing accounts to be used concurrently, not requiring complex passwords, and not changing the passwords sufficiently.

Recommendation No. 8
Treasurer-Tax Collector should restrict user log-on, implementing password filters to provide more password complexity, and setting the password uniqueness to twelve passwords.

Treasurer-Tax Collector Management Response:
Concur. This recommendation has been implemented except for restricting a user from logging on multiple times. Our current system configuration requires a multiple log-on for automated batch processes central to the daily operation of Quantum. Treasury management will contact the vendor to explore alternatives to our current configuration.

Audit Objective #3 – Access and Transmission Controls for EFT Payment Files
Our objective was to review controls over access and transmission of the EFT payment files transmitted to Wells Fargo Bank to ensure the files are adequately protected. These files reside at the Treasurer-Tax Collector server, the Auditor-Controller/CAPS+ file transfer protocol (FTP) server, and OC Enterprise Data Center FTP server.

EFT Payment File Control Strengths
Our audit disclosed that controls over access and transmission of the EFT files transmitted to Wells Fargo Bank are adequately protected. Controls strengths include:

- ✓ File Transfer Protocol (FTP) server accounts were not created for operational users. Users transmitted files to the FTP server via system software preventing users from accessing the FTP server directly.
- ✓ The firewall controls access to the OC Enterprise Data Center FTP server by limiting network traffic to HTTP, HTTPS and RDP protocols.
- ✓ Access to FTP servers is limited to those requiring access to the server.
- ✓ Access to scripts that transmit files is limited to those requiring access.

- ✓ File transfers are performed using Valicert software requiring client software, user id, and password.

- ✓ File transfers are encrypted during transmission to the OC Enterprise Data Center FTP server and Wells Fargo Bank.

The following is where controls can be improved to enhance EFT payment file controls:

Finding No. 9 – Remove Unnecessary CAPS+ FTP Server Administrative Accounts (Control Finding)

We reviewed access to the Auditor-Controller/CAPS+ FTP server and noted several administrative user accounts for individuals who no longer require access to the operating system. These accounts were needed for implementing the CAPS+ financial system and for a limited post go-live period. Unnecessary accounts increase the risk that they may be used inappropriately including altering the EFT files.

Recommendation No. 9
Auditor-Controller should remove any user accounts no longer needed to maintain the CAPS+ hardware/software.

Auditor-Controller Management Response:
Concur. User accounts that are not needed to maintain the CAPS+ hardware/software will be removed.

Finding Nos. 10 and 11 – Remove Unnecessary and Restrict OC Enterprise Data Center FTP Server Administrative Accounts (Two Control Findings)

We identified several accounts with administrator privileges for individuals who no longer require access to the FTP server located at the OC Enterprise Data Center. In addition, there are multiple system accounts (one for each FTP batch job) with administrator privileges (required to transmit files to Wells Fargo Bank). Because these accounts do not have individuals associated with them, there is an increased risk that the accounts may be used inappropriately to alter the EFT files. As such, these accounts require additional controls to limit their log-on capabilities.

Recommendation No. 10
CEO/IT should remove those administrative accounts for individuals no longer requiring access to the FTP server located at the OC Enterprise Data Center.

CEO/IT Management Response:
Concur with Recommendation. The Flagged accounts have been either disabled or deleted. CEO/IT has confirmed that the finding has been remediated as of 6/10/2010.

Recommendation No. 11
CEO/IT should limit the FTP job accounts' log-on capabilities: 1) to the console by removing their RDP (remote access) capabilities and 2) restricting access to specific hours when the account is used to transfer its file.

CEO/IT Management Response:
Concur with Recommendation. CEO/IT has tested how to restrict access to particular hours. CEO/IT will schedule an RFC to impose the logon restrictions. CEO/IT has confirmed that the finding has been remediated as of 8/11/2010.

Finding Nos. 12, 13, and 14 – Disallow Generic FTP External Firewall Rule, Consider Consolidation, and Develop Standardized Policy (Three Control Findings)

The external firewall allows FTP network traffic as a global/generic rule which allows any computer connected to the County's network to send and receive files using FTP.

At a minimum, the FTP network traffic should only be allowed for specific authorized Internet Protocol (IP) addresses rather than as a global rule. Requiring a specific IP address helps ensure the file transfer is made to a known and pre-authorized external destination/source.

Additionally, departments/agencies can process their FTP files directly to the external recipient/sender and bypass the FTP server located at the OC Enterprise Data Center (OCEDC). (See page 5 above – FTP Server (Department/Agency). For example, OC Community Resources and Treasurer-Tax Collector process their banking FTP files directly from the departmental server whereas A-C/CAPS+, Social Services Agency, and Child Support Services process their banking FTP files via the FTP server at the OCEDC.

Files processed directly by the departments/agencies may not take advantage of centralized/unified security features and practices offered by the OCEDC FTP server and the OCEDC facility.

Because of the materiality and inherent vulnerabilities of EFT transactions, CEO/IT should work with the applicable departments/agencies to consider consolidating their FTP activity to the OCEDC FTP server. Consolidation may also help the disaster recovery efforts/coordination. Consideration should be given to:

- Establishment of a single Countywide policy and standardized procedures/tools for administration of the FTP process to reduce the variability of external file transfer processes. Priority should be given to the banking FTPs.
- Development of a centralized inventory of external FTP file transfers (including segregating inbound vs. outbound files).
- Development of a single/centralized schedule for the FTP jobs.
- Identification of sensitive files to employ County standard encryption and other appropriate measures.
- Implementation of any additional FTP servers by the departments/agencies should require the CEO/IT (Chief Information Security Officer – CISO) review and approval.

Recommendation No. 12
CEO/IT should remove the global/generic FTP rule for network traffic through the external firewall. At a minimum, the banking related FTP activity should be the priority.

CEO/IT Management Response:
Concur with Recommendation.

1. This is to support the agency-vendors and customers with controlled access, where each authorized user ID and password must be first approved and set up. This facilitates only secured-non-client based FTP utilizing a browser mechanism. The FTP user must have a User Account and Password to logon, so this is secured. This is not a standard Web Service, simply a mechanism to allow a FTP user to log on without client software.

2. CEO/IT regularly reviews and analyzes logs to restrict outside access. CEO/IT confirms that the finding has been addressed as of 6/10/2010.

Recommendation No. 13
CEO/IT should work with the applicable departments/agencies to consider consolidating external FTP activity to the OC Enterprise Data Center FTP server.

CEO/IT Management Response:
Concur with Recommendation. CEO/IT will with the respective Agencies to look at the feasibility of implementing a secure, consolidated external FTP server.

Recommendation No. 14
CEO/IT should also develop a single Countywide policy for administration of the FTP activity. The policy should consider including: standardized procedures/tools for administration of the FTP process; a requirement for CEO/IT (CISO) review of new FTP servers, maintenance of a centralized inventory of external FTP file transfers; maintenance of a single/centralized schedule for the FTP jobs; and identification of sensitive files.

CEO/IT Management Response:
Concur with Recommendation. CEO/IT – CISO will work with the agencies to develop a single countywide policy for administration of the FTP process. We expect to have a policy in place by 12/31/2010.

Audit Objective #4 - Process Efficiency/Effectiveness
Our objective was to determine if business processes are efficient and effective (no backlogs, duplication of work, or manual processes that could benefit from automation) as related to EFTs in the Auditor-Controller and Treasurer-Tax Collector.

Finding No. 15 – Importance of Quality Assurance Reviews (Control Finding)
Our audit noted a trend by the Auditor-Controller to rely more on department/agency reviews and approvals and to perform less reviews in A-C Claims & Disbursing of lower dollar invoices.

1. Current procedures in A-C Claims & Disbursing require Payment Auditors to review and approve all department/agency invoices regardless of the amount (except those with Satellite Accounting and interface transactions). No additional supervisory review is required for invoices under $100,000. This poses some risk that authorized payments could be initiated and approved at this level without being detected by supervisory review. Because of the high volume of invoices processed, A-C Claims established this review threshold to help improve efficiency in processing payments.

2. In April 2010, the A-C issued a memo to all Agency/Department Heads that central accounts payable staff (A-C Claims & Disbursing) will reduce the level of effort on reviewing certain payments below $5,000 per invoice. This change occurred due to reported resource constraints and to increase focus on cost effectiveness.

3. It came to our attention that A-C Claims & Disbursing is backlogged in their invoice processing due to staff being on leave, a vacant position, and increased processing time needed to enter payments into CAPS+. As a result, staff in the A-C Claims' Compliance Unit have been temporarily assigned to processing invoices.

4. Quality Assurance Reviews (QARs) are performed by the A-C Claims' Compliance Unit as a means to ensure A-C Claims & Disbursing and A-C Satellite Accounting are correctly reviewing and approving department/agency payment requests. The last QAR was conducted on FY 07/08 payments. Because of staffing issues, the QARs have not been assigned a high priority to complete.

In regards to the above, we understand the need for the A-C to monitor its cost effectiveness in processing and approving payment requests; however, as a result, they are relying more on department/agency approvals, and accepting the risk that some of the lower dollar claims could be improper or not properly authorized.

As such, we believe it is especially important to maintain the QAR process as a means for management to monitor the effectiveness, compliance, and propriety of claims processed centrally and in A-C Satellite Accounting. The process should be enhanced to ensure it is completed at least annually, and contains transactions noted above that do not require additional supervisory review in A-C Claims & Disbursing and transactions received as interfaces with CAPS+.

Recommendation No. 15

Auditor-Controller Claims & Disbursing should continue performing annual Quality Assurance Reviews and enhance the review process to include lower dollar EFT payment requests and interface transactions to help detect any improper or non-compliant transactions.

Auditor-Controller Management Response:

Concur. The Auditor-Controller's Office agrees with the importance of Quality Assurance Reviews. We are currently reviewing options to perform these reviews. Additionally, Auditor-Controller/Internal Audit is assisting in evaluating the sampling criteria. The assessment and updated procedures are estimated to be completed by March 31, 2011.

ATTACHMENT A: Report Item Classifications

For purposes of reporting our audit observations and recommendations, we will classify audit report items into three distinct categories:

Material Control Weaknesses:
A serious audit finding or a combination of Significant Control Weakness that can result in financial liability and exposure to a department/agency and/or to the County as a whole. Management is expected to address "Material Weaknesses" brought to their attention immediately.

Significant Control Weaknesses:
Audit findings or a combination of Control Findings that represent a significant deficiency in the design or operation of internal controls. Significant Issues generally will require prompt corrective actions.

Control Findings:
Audit findings concerning internal controls, compliance issues, or efficiency/effectiveness issues that require management's corrective action to implement or enhance processes and internal controls. Control Findings are expected to be addressed within our follow-up process of six months, but no later than twelve months.

ATTACHMENT B: Auditor-Controller Management Responses

AUDITOR-CONTROLLER
COUNTY OF ORANGE

HALL OF FINANCE AND RECORDS
12 CIVIC CENTER PLAZA, ROOM 200
POST OFFICE BOX 567
SANTA ANA, CALIFORNIA 92702-0567

(714) 834-2450 FAX: (714) 834-2569

www.ac.ocgov.com

DAVID E. SUNDSTROM, CPA
AUDITOR-CONTROLLER

SHAUN M. SKELLY
CHIEF DEPUTY
AUDITOR-CONTROLLER

JAN E. GRIMES
DIRECTOR
CENTRAL ACCOUNTING OPERATIONS

WILLIAM A. CASTRO
DIRECTOR
SATELLITE ACCOUNTING OPERATIONS

PHILLIP T. DAIGNEAU
DIRECTOR
INFORMATION TECHNOLOGY

October 12, 2010

TO: Peter Hughes, Director
Internal Audit Department

SUBJECT: Response – Internal Control Audit $22 Billion Electronic Funds Transfer Processes, Audit No. 2821

The following are our responses to the recommendations contained in the Internal Control Audit $22 Billion Electronic Funds Transfer Processes, Audit No. 2821.

Recommendation No. 1
Auditor-Controller ensure its Satellite Accounting Units verify the payment approval with the corresponding agency's authorized signature forms/access request forms prior to processing EFT payments.

Auditor-Controller Response:
Concur. Satellite Accounting Units will be reminded when processing EFT payments to always check the validity of the agency's authorized signer to the CAPS+ Access Request form and to only process EFT requests signed by an authorized signer. Additionally, written procedures are estimated to be completed by March 31, 2011.

Recommendation No. 2
Auditor-Controller Check Writing ensure that hard copy EFT/On Demand Wire Forms contain authorized signatures before releasing payments.

Auditor-Controller Response:
Concur. Check Writing will be reminded to review for authorized signature prior to submitting the document in CAPS+. Additionally, written procedures are estimated to be completed by December 30, 2010.

ATTACHMENT B: Auditor-Controller Management Responses (continued)

Peter Hughes, Director, Internal Audit Department
October 12, 2010
Page 2

Recommendation No. 3
Auditor-Controller Claims & Disbursing ensure payment processors adequately review the data entered against supporting documentation, including vendor addresses, to ensure it is accurate and complete prior to processing payments.

Auditor-Controller Response:
Partially concur. Payment processors do review supporting documentation to ensure accuracy, but they do not audit account coding. It is the responsibility of the submitting department to ensure that account coding is correct. Additionally, we agree that all "miscellaneous trust" vendor payments must have a payee/vendor name. Check Writing will be reminded to review the input of the vendors name prior to submitting the GA Trust Fund Payment document. Additionally, written procedures are estimated to be completed by December 30, 2010.

Recommendation No. 4
Auditor-Controller should evaluate if standardized policies and procedures for authorizing and approving disbursements can be established to ensure they are consistently applied both in A-C Claims and Disbursing and the A-C Satellite Accounting Units. The standardized procedures should include scope of reviews and specific review criteria that can be incorporated into department/agency policy and procedures.

Auditor-Controller Response:
Concur. Auditor-Controller will be developing uniform guidelines and criteria for reviewers to follow and anticipated completion date is March 31, 2011.

Recommendation No. 5
Auditor-Controller should also evaluate whether disbursements processed as department interfaces should be subject to Auditor-Controller review and approval thresholds described above, and if support documentation should be required as part of the review process.

Auditor-Controller Response:
Concur. Department interfaces will be evaluated as part of reviewing the scope of Quality Assurance testing which is part of Recommendation No. 15 and is estimated to be completed by March 31, 2011.

Recommendation No. 6
Auditor-Controller Claims & Disbursing Unit and Satellite Accounting Offices ensure during their review that bank account codes and ABA numbers are correctly documented prior to approving EFTs.

ATTACHMENT B: Auditor-Controller Management Responses (continued)

Auditor-Controller Response:
Concur. Auditor-Controller Claims will remind Central Operations and Satellite Accounting Offices to review and ensure accuracy of these numbers. Additionally, written procedures are estimated to be completed by March 31, 2011.

Recommendation No. 9

Auditor-Controller should remove any user accounts no longer needed to maintain the CAPS+ hardware/software.

Auditor-Controller Response:

Concur. User accounts that are not needed to maintain the CAPS+ hardware/software will be removed.

Recommendation No. 15
Auditor-Controller Claims & Disbursing should continue performing annual Quality Assurance Reviews and enhance the review process to include lower dollar EFT payment requests and interface transactions to help detect any improper or non-compliant transactions.

Auditor-Controller Response:
Concur. The Auditor-Controller's Office agrees with the importance of Quality Assurance Reviews. We are currently reviewing options to perform these reviews. Additionally, Auditor-Controller/Internal Audit is assisting in evaluating the sampling criteria. The assessment and updated procedures are estimated to be completed by March 31, 2011.

David E. Sundstrom
Auditor-Controller

VR:lr (EFT Audit Response2/wg-lr)

cc: Mike Goodwin, Senior Audit Manager, Internal Audit Department
Shaun Skelly, Chief Deputy Auditor-Controller
Bill Castro, Director, Satellite Accounting Operations
Jan Grimes, Director, Central Accounting Operations
Victoria Ross, A/C - Claims and Disbursing Manager

ATTACHMENT C: Treasurer-Tax Collector Management Responses

OFFICE OF THE TREASURER-TAX COLLECTOR

HALL OF FINANCE & RECORDS
11 CIVIC CENTER PLAZA, SUITE G76
POST OFFICE BOX 4515
SANTA ANA, CA 92702
www.ttc.ocgov.com

CHRISS W. STREET
TREASURER-TAX COLLECTOR

PAUL C. GORMAN, C.P.A., CTP, CPFIM
CHIEF ASSISTANT TREASURER-TAX COLLECTOR

JENNIFER BURKHART, CFA
ASSISTANT TREASURER-TAX COLLECTOR

ROBIN RUSSELL
ASSISTANT TREASURER-TAX COLLECTOR
ADMINISTRATION

October 8, 2010

Dr. Peter Hughes
Director, Internal Audit
County of Orange
12 Civic Center Plaza, Room 232
Santa Ana, CA 92701

RECEIVED
INTERNAL AUDIT DEPARTMENT
2010 OCT 12 PM 2:22

Dear Dr Hughes:

Pursuant to Audit Oversight Committee Administrative Procedure No. 1, we have prepared our response to the Draft Report on Internal Control Audit of Auditor-Controller's and Treasurer-Tax Collector's $22 Billion Electronic Funds Transfer Processes. The recommendation numbers used in your report reference our response.

Internal Audit Finding No. 7 – Remove CEO System EFT "Release" Role for EFT Manual Approvers (Control Finding)

Commercial Electronic Office (CEO) system controls prevent users from creating and releasing (approving/release) their own transactions. The T-TC has also implemented a manual approval of the EFT after it has been created and before it has been released in CEO. Two individuals in the T-TC who are manual approvers of EFTs were also given the ability to "release" EFTs in the CEO system. The system "release" access was granted as an emergency back-up. Good internal controls require proper segregation of these duties. As there appears to be a sufficient number of users with "release" authority, the "release" access granted to the two manual approvers should be removed.

Recommendation No. 7
Treasurer-Tax Collector should remove the "release" access within the CEO system for the two manual approvers of EFTs.

Treasurer-Tax Collector Management Response:
Concur. This recommendation has been implemented.

Page 1 of 2

ATTACHMENT C: Treasurer-Tax Collector Management Responses (continued)

Dr. Peter Hughes
October 8, 2010

Internal Audit Finding No. 8 – More Restrictive Quantum Account and Password Settings (Control Finding)

The Quantum application security was configured to allow a user to log-on multiple times, the password filters did not provide for any password complexity, and password uniqueness was set to "one" password. These settings provide for easier user administration. However, these settings do not conform with best practices. These settings increase the probability that an account may be used inappropriately by allowing accounts to be used concurrently, not requiring complex passwords, and not changing the passwords sufficiently.

Recommendation No. 8
Treasurer-Tax Collector should restrict user log-on, implementing password filters to provide more password complexity, and setting the password uniqueness to twelve passwords.

Treasurer-Tax Collector Management Response:
Concur. This recommendation has been implemented except for restricting a user from logging on multiple times. Our current system configuration requires a multiple log-on for automated batch processes central to the daily operation of Quantum. Treasury management will contact the vendor to explore alternatives to our current configuration.

If you have additional questions or follow-up comments; please contact me at 834-2288.

Very truly yours,

Paul C. Gorman
Chief Assistant Treasurer-Tax Collector

Page 2 of 2

ATTACHMENT D: CEO/Information Technology Management Responses (Continued)

County Executive Office
Memorandum

September 30, 2010

To: Autumn Mckinney, Senior Audit Manager

From: KC Roestenberg, Director, Business IT Shared Services

Subject: CEO-IT Action Items in Response to Audit Report - 2948

The purpose of this memorandum is to follow up on a previous draft response submitted to County Internal Audit on 06/10/2010. Below are CEO/IT NPS responses for each point in scope. The applicability of scope was determined by Internal Auditor.

CEO/IT NPS has already implemented number corrective and compensating measures when such actions were timely or warranted.

CEO/IT greatly appreciates the support and cooperation of IAD and the client-agency staff in maintaining and strengthening effective internal and management controls.

Please do not hesitate to contact me directly if you have any questions or concerns.

Sincerely,
KC Roestenberg

cc:
Satish Ajmani
Joel Manfredo
Mahesh Patel
Mark Khanlar
Tony Lucich
Gary Mills

1

ATTACHMENT D: CEO/Information Technology Management Responses (Continued)

Detailed CEOIT Response for IAD Findings:

Finding Nos. 10 and 11 – Remove Unnecessary and Restrict OC Enterprise Data Center FTP Server Administrative Accounts (Two Control Findings)

We identified several accounts with administrator privileges for individuals who no longer require access to the FTP server located at the OC Enterprise Data Center. In addition, there are multiple system accounts (one for each FTP batch job) with administrator privileges (required to transmit files to Wells Fargo Bank). Because these accounts do not have individuals associated with them, there is an increased risk that the accounts may be used inappropriately to alter the EFT files. As such, these accounts require additional controls to limit their log-on capabilities.

Recommendation No. 10
CEO/IT should remove those administrative accounts for individuals no longer requiring access to the FTP server located at the OC Enterprise Data Center.

CEO/IT Management Response: Concur with Recommendation
The flagged accounts have been either disabled or deleted. CEO/IT has confirmed that the finding has been remediated as of 6/10/2010.

Recommendation No. 11
CEO/IT should limit the FTP job accounts' log-on capabilities: 1) to the console by removing their RDP (remote access) capabilities and 2) restricting access to specific hours when the account is used to transfer its file.

CEO/IT Management Response: Concur with Recommendation
CEO/IT has tested how to restrict access to particular hours. CEO/IT will schedule an RFC to impose the logon restrictions. CEO/IT has confirmed that the finding has been remediated as of 8/11/2010.

Finding Nos. 12, 13, and 14 – Disallow Generic FTP External Firewall Rule, Consider Consolidation, and Develop Standardized Policy (Three Control Findings)

The external firewall allows FTP network traffic as a global/generic rule which allows any computer connected to the County's network to send and receive files using FTP.

At a minimum, the FTP network traffic should only be allowed for specific authorized Internet Protocol (IP) addresses rather than as a global rule. Requiring a specific IP address helps ensure the file transfer is made to a known and pre-authorized external destination/source.

Additionally, departments/agencies can process their FTP files directly to the external recipient/sender and bypass the FTP server located at the OC Enterprise Data Center

2

ATTACHMENT D: CEO/Information Technology Management Responses (Continued)

(OCEDC). (See page 7 above – FTP Server (Department/Agency). For example, OC Community Resources and Treasurer-Tax Collector process their banking FTP files directly from the departmental server whereas A-C/CAPS+, Social Services Agency, and Child Support Services process their banking FTP files via the FTP server at the OCEDC.

Files processed directly by the departments/agencies may not take advantage of centralized/unified security features and practices offered by the OCEDC FTP server and the OCEDC facility.

Because of the materiality and inherent vulnerabilities of EFT transactions, CEO/IT should work with the applicable departments/agencies to consider consolidating their FTP activity to the OCEDC FTP server. Consolidation may also help the disaster recovery efforts/coordination. Consideration should be given to:

- Establishment of a single countywide policy and standardized procedures/tools for administration of the FTP process to reduce the variability of external file transfer processes. Priority should be given to the banking FTPs.
- Development of a centralized inventory of external FTP file transfers (including segregating inbound vs. outbound files).
- Development of a single/centralized schedule for the FTP jobs.
- Identification of sensitive files to employ County standard encryption and other appropriate measures.
- Implementation of any additional FTP servers by the departments/agencies should require the CEO/IT (Chief Information Security Officer – CISO) review and approval.

Recommendation No. 12
CEO/IT should remove the global/generic FTP rule for network traffic through the external firewall. At a minimum, the banking related FTP activity should be the priority.

CEO/IT Management Response: Concur with Recommendation

1. This is to support the agency-vendors and customers with controlled access, where each authorized user ID and password must be first approved and set up. This facilitates only secured non-client based FTP utilizing a browser mechanism. The FTP user must have a User Account and Password to logon, so this is secured. This is not a standard Web Service, simply a mechanism to allow a FTP user to log on without client software.
2. CEO/IT regularly reviews and analyzes logs to restrict outside access.

CEO/IT confirms that the finding has been addressed as of 6/10/2010.

3

ATTACHMENT D: CEO/Information Technology Management Responses (Continued)

Recommendation No. 13
CEO/IT should work with the applicable departments/agencies to consider consolidating external FTP activity to the OC Enterprise Data Center FTP server.

CEO/IT Management Response: Concur with Recommendation
CEO/IT will with the respective Agencies to look a the feasibility of implementing a secure, consolidated external FTP server.

Recommendation No. 14
CEO/IT should also develop a single countywide policy for administration of the FTP activity. The policy should consider including: standardized procedures/tools for administration of the FTP process; a requirement for CEO/IT (CISO) review of new FTP servers, maintenance of a centralized inventory of external FTP file transfers; maintenance of a single/centralized schedule for the FTP jobs; and identification of sensitive files.

CEO/IT Management Response: Concur with Recommendation
CEO/IT - CISO will work with the agencies to develop a single countywide policy for administration of the FTP process. We expect to have a policy in place by 12/31/2010.

4