AGENDA ITEM # 6
February 11, 2014

6. REPORTS TO BE RECEIVED FOR FILING:

a. Division of Inspector General, Audit Services, Clerk of the Circuit Court and Comptroller, 2014 Annual Audit Plan.

b. Division of Inspector General, Audit Services, Clerk of the Circuit Court and Comptroller, Report No. 2014-01, January 16, 2014 – Follow-Up Audit of Enterprise Information Security Oversight and Administration.

c. Division of Inspector General, Audit Services, Clerk of the Circuit Court and Comptroller, Report No. 2014-02, January 16, 2014 – Follow-Up Audit of the Management of Cross Bar and AL-Bar Ranches.

d. Dock Fee Report for the month of December 2013.

e. Quarterly Report of Routine Dock and Dredge/Fill Permits issued from October 1, 2013 to December 31, 2013.

Ken Burke, CPA
CLERK OF THE CIRCUIT COURT AND COMPTROLLER
PINELLAS COUNTY, FLORIDA

Clerk of the County Court
Recorder of Deeds
Clerk and Accountant of the Board of County Commissioners
Custodian of County Funds
County Auditor

Division of Inspector General
510 Bay Avenue
Clearwater, FL 33756
Telephone: (727) 464-8371
Fax: (727) 464-8386
Fraud Hotline: (727) 45FRAUD (453-7283)
Clerk's website: www.mypinellasclerk.org

TO: The Honorable Chairman and Members of the Board of County Commissioners

FROM: Ken Burke, CPA
Clerk of the Circuit Court and Comptroller
Ex Officio County Auditor

SUBJECT: Follow-Up Audit of Pinellas County Enterprise Information Security & Oversight Administration

DATE: January 16, 2014

For your review and filing in the Official Records, I am enclosing a copy of the follow-up audit dated January 16, 2014 on the above-referenced audit.

I hope you find this report helpful in ensuring Pinellas County government provides the best possible service to our citizens.

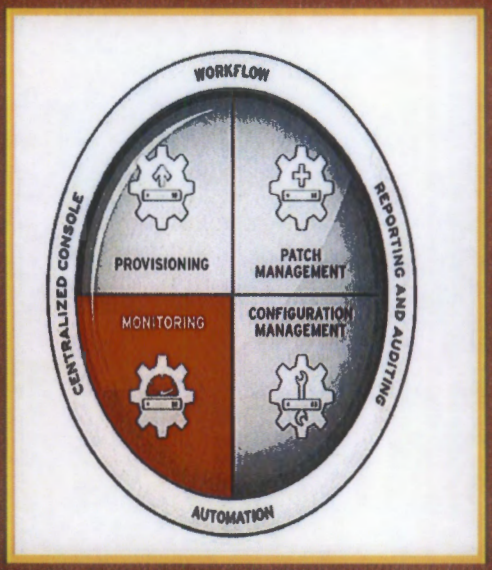
cc: Robert S. LaSala, County Administrator
Martin Rose, Chief Information Officer, Business Technology Services (BTS)
Jim Russell, Assistant Executive Director, Business Technology Services
Thomas Fredrick, BTS Senior Manager
Jeff Rohrs, BTS Principal Enterprise Architect
Jim Bennett, County Attorney
Claretha N. Harris, Chief Deputy Director, Finance Division
Crowe Horwath

An Accredited Office of Inspectors General

DIVISION OF INSPECTOR GENERAL

KEN BURKE, CPA
CLERK OF THE CIRCUIT COURT AND COMPTROLLER
PINELLAS COUNTY, FLORIDA

FOLLOW-UP AUDIT OF ENTERPRISE INFORMATION SECURITY OVERSIGHT AND ADMINISTRATION



FLORIDA LAW ENFORCEMENT ACCREDITATION COMMISSION

An Accredited Office of Inspectors General

Hector Collazo Jr.
Inspector General/Chief Audit Executive

Audit Team
Ken Green, CIGA – Inspector General Manager
Flo Riggie, CIA, CIGA, CISA, CRISC, ITIL-F – Inspector General Auditor II

JANUARY 16, 2014
REPORT NO. 2014-01

Ken Burke, CPA
CLERK OF THE CIRCUIT COURT AND COMPTROLLER
PINELLAS COUNTY, FLORIDA

Clerk of the County Court
Recorder of Deeds
Clerk and Accountant of the Board of County Commissioners
Custodian of County Funds
County Auditor

Division of Inspector General
510 Bay Avenue
Clearwater, FL 33756
Telephone: (727) 464-8371
Fax: (727) 464-8386
Fraud Hotline: (727) 45FRAUD (453-7283)
Clerk's website: www.mypinellasclerk.org

January 16, 2014

The Honorable Chairman and Members
of the Board of County Commissioners

We have conducted a Follow-Up Audit of the Pinellas County Enterprise Information Security Oversight and Administration. The objectives of our review were to determine the implementation status of our previous recommendations.

Of the two recommendations contained in the audit report, we determined that both have been implemented. The status of each recommendation is presented in this follow-up review.

We appreciate the cooperation shown by the staff of Business Technology Services during the course of this review.

Respectfully Submitted,

Hector Collazo Jr.
Inspector General/Chief Audit Executive

Approved:

Ken Burke, CPA*
Clerk of the Circuit Court and Comptroller
Ex Officio County Auditor

*Regulated by the State of Florida

An Accredited Office of
Inspectors General

TABLE OF CONTENTS

INTRODUCTION

Scope and Methodology

We conducted a follow-up audit of the Pinellas County Enterprise Information Security Oversight and Administration functions. The purpose of our follow-up review is to determine the status of previous recommendations for improvement.

The purpose of the original audit was to:

- Interviewed individuals responsible for the administration of the BTS enterprise information security function to obtain a clear understanding of the operations.
- Evaluated the adequacy of policies, procedures, and internal controls over the administration of information security.
- Tested, on a sample basis, the effectiveness of the BTS information security processes.
- Reviewed planning for Fiscal Year 2011-2012 covering security testing of County electronic information access and other related planned reviews.

To determine the current status of our previous recommendations, we surveyed and/or interviewed management to determine the actual actions taken to implement recommendations for improvement. We performed limited testing to verify the process of the recommendations for improvement.

Our follow-up audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and the *Standards for Offices of Inspector General,* and, accordingly, included such tests of records and other auditing procedures, as we considered necessary in the circumstances. Our follow-up testing was performed during the month of October and November 2013. The original audit period was January 1, 2010 to December 31, 2011. However, transactions and processes reviewed were not limited by the audit period.

Overall Conclusion

Of the two recommendations in the report, we determined that both were implemented. We commend management for the implementation of our recommendations.

Status of Action Plan

OFI NO.	PREVIOUS RECOMMENDATION	IMPLEMENTATION STATUS				
		Implemented	Acceptable Alternative	Partially Implemented	Not Implemented	No Longer Applicable
1	***Security For The Newly Implemented OPUS Application Needs To Be Reviewed And Updated For The Current Production Environment.***					
	We recommended management develop formal security policies and procedures for OPUS. Prior to implementation, these document(s) should be reviewed and approved by the BTS Information Security Officer.	✓				
2	***An Overall Application Data Change Policy Is Needed For Non-Mainframe Applications.***					
	Establish a formal policy that BTS application staff not change production data unless there is a change management policy for this task. The change management policy should define procedures for evaluating, authorizing, and submitting service requests for changing production data for each application supported by the BTS department.	✓				

Background

The Pinellas County Information Security Panel (Panel) was formed to protect the information technology assets of Pinellas County taxpayers and its users. The Panel is the single entity that creates, develops, and monitors the Pinellas County Information Security Policy. The BTS Board ratifies policies created by the following Panel members:

- BTS Information Security Officer
- Supervisor of Elections
- Sheriff
- Property Appraiser
- Public Defender
- Chief Judge
- Tax Collector
- Board of County Commissioners (BCC)
- State Attorney
- Clerk of the Circuit Court

The Pinellas County Information Security Policy (Policy) establishes the BTS Information Security Officer that has the authority to take action consistent with the Policy to protect the enterprise network and associated systems. The Policy applies to all Pinellas County agencies, all other agencies that use Pinellas County information and technology, and all third parties who have access to County information and technology.

The application for oversight and administration of enterprise information security is the responsibility of BTS line management. The general areas of responsibility are:

- Enterprise Business Applications
- Infrastructure Services
- Server/Storage/Desktop
- Oracle Applications

The functionality includes daily operations, planning, development, evaluation of new products, and security issues. Vulnerability assessments and other evaluations and testing are coordinated by the Security Officer's department. Best practices have been established for key technology areas and are posted on the BTS website. An enterprise vulnerability assessment is scheduled for 2012, with the last assessment performed by Westin Engineering, Inc. in 2006.

STATUS OF RECOMMENDATIONS

This section reports our follow-up on actions taken by management on the Recommendations for Improvement in our original audit of the Pinellas County Enterprise Information Security Oversight and Administration. The recommendations contained herein are those of the original audit, followed by the current status of the recommendations.

1. Security For The Newly Implemented OPUS Application Needs To Be Reviewed And Updated For The Current Production Environment.

The security process for the Oracle Project Unified Solution (OPUS) application needs additional refinement for the production environment. The application business structure roles and responsibilities are in place and cross validation rules are established. An independent evaluation of the application security is being performed by Sunera, LLC, a management and information technology consulting firm. When the independent evaluation is completed, BTS management will address the recommendations and put in place required changes. Upon completion of this process, BTS should develop a formal internal security process and related procedures for the OPUS application that includes reports and ongoing monitoring.

Implementation of the phases of the OPUS application has been ongoing throughout 2011. As each module of the application was put into production, security settings were configured. Some business issues are still being addressed.

The implementation of a security process and related procedures will reduce inherent security risks that exist within any application and formalize the process. There should be formal standards and procedures for managing and monitoring OPUS security options that are available through the application.

We Recommended management:

Develop formal security policies and procedures for OPUS. Prior to implementation, these document(s) should be reviewed and approved by the BTS Information Security Officer.

Status:

Implemented. A policy for requesting or changing access and documenting all security access has been developed and implemented.

2. An Overall Application Data Change Policy Is Needed For Non-Mainframe Applications.

There is no BTS policy that clearly states that BTS application staff should not alter application production data without following an established change management procedure. BTS staff is assigned to applications with the BTS staff member having administrator rights to the application. The BTS staff may also have access to the production data for their assigned application. Limiting access to production data by the BTS staff with administration rights to that application, in most cases, is not a system option for applications that run in a non-mainframe environment.

The Inspector General conducted and issued Investigative Report I-2011-02 which concluded that BTS staff were changing production data in the Permits Plus application. When the production data was changed, there was no change management procedure for the application; a change management procedure has since been established by BTS and the data owner.

The risk of BTS staff altering production data is limited to applications that BTS staff members have administration rights to and have the access rights to the database. This risk will only be present if there is no application specific established change management policy that defines procedures for evaluating, authorizing, and submitting service requests.

There should be a clear separation of duties or a formal procedure requiring the data owner management to request a change of production data in an application database that is not processed through the normal functioning of that application.

We Recommended management:

Establish a formal policy that BTS application staff not change production data unless there is a change management policy for this task. The change management policy should define procedures for evaluating, authorizing, and submitting service requests for changing production data for each application supported by the BTS department.

Status:

Implemented. A formal change policy has been developed. The policy defines the procedure for evaluating, authorizing, and submitting service requests for changes to production data.

Division of Inspector General

Ken Burke, CPA

Clerk of the Circuit Court
& Comptroller
Pinellas County, Florida

Services Provided

Audit Services
Investigations
Guardianship Services
Consulting
Training
Guardianship Fraud Hotline
County Fraud Hotline

An Accredited Office of
Inspectors General

Call: (727) 45FRAUD
(727) 453-7283
Fax: (727) 464-8386
Internet: www.mypinellasclerk.org
www.twitter.com/pinellasig
www.facebook.com/igpinellas

Write:
Fraud Hotline
Public Integrity Unit
Division of Inspector General
510 Bay Avenue
Clearwater, FL 33756