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

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

SUBJECT: Audit of Enterprise Information Security Oversight & Administration

DATE: July 12, 2012

For your review and filing in the Official Records, I am enclosing a copy of the report dated July 12, 2012 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
Mark Woodard, Assistant County Administrator
Jim Bennett, County Attorney
Paul F. Alexander, Director, BTS
Jim Russell, Assistant Executive Director, BTS
Jeff Rohrs, Chief Technologist, BTS
Claretta N. Harris, Chief Deputy Director, Finance Division
Ernst & Young
DIVISION OF INSPECTOR GENERAL
Ken Burke, CPA
Clerk of the Circuit Court
Pinellas County, Florida

AUDIT OF ENTERPRISE INFORMATION
SECURITY OVERSIGHT & ADMINISTRATION

Hector Collazo, Jr., Director
Inspector General/Chief Audit Executive

Audit Team
Ronald Peters CIA, CISA, CIGA – Senior Inspector General Auditor

JULY 12, 2012
REPORT NO. 2012-09
July 12, 2012

The Honorable Chairman and Members
of the Board of County Commissioners

We have conducted an audit of the Enterprise Information Security Oversight & Administration. Our audit objectives were to:

1. Evaluate the Business Technology Services (BTS) structure related to the authority, control, and oversight of the enterprise information security for Pinellas County.
2. Ensure there is a suitable set of internal controls to protect against threats and vulnerabilities for the enterprise information environment.
3. Ensure that internal controls are established, implemented, monitored, and reviewed for improvement.

We conclude that:

- The administration and oversight for the County enterprise information security is adequate. The utilization of the BTS management structure to perform security functions in the daily operations, planning and development, and new product function is cost effective.
- The Pinellas County Security Policies are adequate and effective in reducing risk in the enterprise environment. Best practices are in place and being utilized to reduce vulnerabilities.
- The BTS management functions ensure continuous evaluation and improvement in the County information security structure. In addition, the Information Security Panel representatives function as an oversight and monitoring device for changes in technology and state of the art security exposure evaluations.

Opportunities for Improvement are presented in this report.
We appreciate the cooperation shown by the staff of the BTS Enterprise Information Security Oversight and Administration during the course of this review. We commend management for their responses to our recommendations.

Respectfully Submitted,

Hector Collazo, Jr., Director
Division of Inspector General

Approved:

Ken Burke, CPA*
Clerk of the Circuit Court
Ex Officio County Auditor
*Regulated by the State of Florida
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Opportunities for Improvement</td>
<td></td>
</tr>
<tr>
<td>1. <em>Security For The Newly Implemented OPUS Application Needs To Be Reviewed And Updated For The Current Production Environment.</em></td>
<td>9</td>
</tr>
<tr>
<td>2. <em>An Overall Application Data Change Policy Is Needed For Non-Mainframe Applications.</em></td>
<td>10</td>
</tr>
</tbody>
</table>
INTRODUCTION

Synopsis

The administration and oversight functions performed by Business Technology Services (BTS) for Pinellas County enterprise information security adequately covers exposure to inherent risk. Best practices have been adopted along with County security policies by the enterprise information technology users. Ongoing technology issues are addressed by the Information Security Panel.

Scope and Methodology

We conducted an audit of the Pinellas County Enterprise Information Oversight and Administration functions.

In order to meet our objectives we:

- 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.

We performed such other audit procedures that we considered necessary in the circumstances.

The objectives of the audit were to:

1. Evaluate the BTS structure related to the authority, control, and oversight of the enterprise information security for Pinellas County.
2. Ensure there is a suitable set of internal controls to protect against threats and vulnerabilities for the enterprise information environment.
3. Ensure that internal controls are established, implemented, monitored, and reviewed for improvement.

Our audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing and the Principles and Standards for Offices of Inspector General, and accordingly, included such tests of records and other auditing procedures, as we considered necessary in the circumstances. The audit period was January 1, 2010 to December 31, 2011. However, processes reviewed were not limited by the audit period.
**Overall Conclusion**

We conclude:

- The administration and oversight for the County enterprise information security was adequate. The utilization of the BTS management structure to perform security functions in the daily operations, planning and development, and new product function is cost effective.

- The Pinellas County Security Policies are adequate and effective in reducing risk in the enterprise environment. Best practices are in place and being utilized to reduce vulnerabilities.

- The BTS management functions ensure continuous evaluation and improvement in the County information security structure. In addition, the Information Security Panel representatives function as an oversight and monitoring device for changes in technology and state of the art security exposure evaluations.
# Action Plan

<table>
<thead>
<tr>
<th>FINDING NO.</th>
<th>FINDING (CAPTION) RECOMMENDATIONS</th>
<th>MANAGEMENT RESPONSES</th>
<th>IMPLEMENTATION STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Security For The Newly Implemented OPUS Application Needs To Be Reviewed And Updated For The Current Production Environment.</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><strong>An Overall Application Data Change Policy Is Needed For Non-Mainframe Applications.</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.
OPPORTUNITIES FOR IMPROVEMENT

Our audit disclosed certain policies, procedures, and practices that could be improved. Our audit was neither designed nor intended to be a detailed study of every relevant system, procedure, or transaction. Accordingly, the Opportunities for Improvement presented in this report may not be all-inclusive of areas where improvement may be needed.

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 recommend** 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.

**Management Response:**

We concur. BTS is in the process of addressing the recommendations from the Sunera independent assessment. In addition, BTS is currently in the RFP (Request For Proposals) process for an enterprise vulnerability assessment, which will include an assessment of the OPUS production environment.
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 recommend** 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.

**Management Response:**

We concur. BTS Change Management and Enterprise Business Application Services are working on a change to our current processes to formalize the application data change process.
DIVISION OF INSPECTOR GENERAL

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

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

Phone: (727) 453-3728
Fax: (727) 464-8386

Internet: www.mypinellasclerk.org
www.twitter.com/pinellasig
www.facebook.com/igpinellas

Accredited Office of Inspector General
by the Commission for Florida Law Enforcement Accreditation