STATE OF FLORIDA INSPECTORS GENERAL
Governor Rick Scott
Melinda M. Miguel, Chief Inspector General

ENTERPRISE AUDIT PLAN
For Fiscal Year 2012-2013

This plan identifies the enterprise audits and projects to be conducted during Fiscal Year 2012-2013 by participating state agency inspectors general.

Overview of Methodology Used to Determine Areas Selected for Audit and Review

Section 14.32, Florida Statutes, provides that the Governor's Chief Inspector General shall initiate and coordinate activities designed to deter, detect, prevent and eradicate fraud, waste, abuse, and mismanagement in government. Additionally, the Chief Inspector General shall request such assistance as may be necessary to perform the duties of the Chief Inspector General.

The Chief Inspector General asked agency inspectors general to participate in the identification of the enterprise audit topics by meeting with their agency heads and identifying areas of concern with an enterprise impact. Twenty-eight potential audit topics were identified and inspectors general along with audit directors were asked to participate in assessing risk associated with each of those potential projects. The group identified six topics for inclusion in the 2012-2013 enterprise audit plan.

Agency-specific audit projects are addressed in the agency audit plans. To plan for both agency specific audit projects and enterprise projects, each agency inspector general was asked to allocate 20 percent of their direct audit hours to enterprise projects.

Audit Plan for Fiscal Year 2012-2013

Based on the results of the risk assessment, the following areas were identified as enterprise priorities for Fiscal Year 2012-2013. The selected enterprise projects cover administrative issues common to most state agencies and issues specific to agencies with a healthcare focus.

Topic	Type
Assessment of Managed Care Organizations' Anti-Fraud Processes	Multi-agency Team[1]
Background Screenings	Enterprise Project[2]
Computer Security Incident Response Teams	Enterprise Project
Cyber Security	Enterprise Project
Disaster Recovery Plans at Shared Resource Centers	Multi-agency Team
Service Level Agreements with Shared Resource Centers	Multi-agency Team

[1] Multi-Agency Team projects will not involve all agencies but will address issues common to the participating agencies.
[2] Enterprise projects will generally be completed by all agencies.

The preliminary focus of each project is as follows:

Assessment of Managed Care Organizations' Anti-Fraud Processes
- As Managed Care Organizations (MCO's) assume greater roles in healthcare delivery, they are becoming more significant to the State. A major role that the MCOs will begin to assume is the frontline prevention and detection of fraud and abuse. Each Medicaid-participating MCO is required to develop and present anti-fraud plans to both the Department of Financial Services and the Agency for Health Care Administration. We propose to evaluate anti-fraud plans already submitted to assess whether the plans are viable and comport with known fraud risks. The product of the evaluation, while not yet fully defined, is envisioned to be a guide for creation of anti-fraud plans and the identification of best practices.

Background Screenings
- At varying levels, every state agency performs background screenings for employees, contractors and/or providers. We propose to review the current processes used by each state agency in performing this enterprise-wide task to identify opportunities for efficiencies, cost savings and best practices.

Computer Security Incident Response Teams
- Rule 71A-1.014, Florida Administrative Code, provides that each agency shall establish a Computer Security Incident Response Team (CSIRT) to respond to suspected computer security incidents by identifying and controlling the incidents, notifying designated CSIRT responders, and reporting findings to agency management. We propose to evaluate whether agencies have properly established CSIRTs and whether the Teams possess the required technical and procedural skills and resources to appropriately handle computer security incidents. Also, we propose to determine if the Teams have established roles, responsibilities, and communication procedures to respond to computer security incidents which may occur.
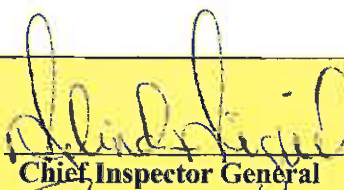
Cyber Security
- This project would inventory state government web applications and assess those applications for specific cyber security vulnerabilities. The product of this assessment, while not yet fully defined, is envisioned to be guidance for state agencies in establishing best practices for cyber security.

Disaster Recovery and Business Continuity Plans at Shared Resource Centers
- A review would be performed to determine the adequacy of the Shared Resource Centers' Disaster Recovery and Business Continuity Plans.

Service Level Agreements with Shared Resource Centers
- A review will be performed of the current Service Level Agreements with the Shared Resource Centers to determine if the agreements adequately address the services to be performed by the Centers and the responsibilities of each party. The review will include an assessment of data maintenance and security.

Respectfully Submitted by: _(signature)_   **Date:** 6-26-12
Chief Inspector General

Audit Plan Approved by: _(signature)_   **Date:** 6-27-12
Governor