Association of Government Accountants – Austin Chapter
Identity Theft – Corporate Risks and Controls by Paul Morris
December 13, 2012 Luncheon

Speaker: Paul Morris, CPA, CGFM
Paul Morris is the DFPS Director of Internal Audit and a liaison to all audit functions and oversight bodies external to DFPS. He is a Certified Public Accountant and Certified Internal Auditor. Mr. Morris was formerly a director of internal audit in the health care industry.

Prior to this, he began his 18 year career in internal audit and health care operations with the University of Texas Houston Health Science Center and the M.D. Anderson Cancer Center. Mr. Morris has 8 years of state service. He is also a Lieutenant Commander in the United States Coast Guard Reserve.

Luncheon Highlights:

A. Personal Identity Theft
   1. Definition: "The deliberate use of another person's name and other identifying information to commit theft or fraud or to access confidential information about an individual." GTAG 5 – Managing and Auditing Privacy Risks, IIA June 2006
   2. 4 Categories of Personal Identity Theft:
      a. Financial Identity Theft – usually to make purchases
      b. Government Identity Theft – usually used as a means to gain employment
      c. Medical Identity Theft – usually used to get medical claims or services
      d. Child Identity Theft

B. How Identity Theft has Evolved with Technology
   1. Assuming the identity of another person is the earliest form of fraud.
   2. Obtaining data through telephone fraud.
   3. The physically collection of data, like dumpster diving.
   4. Obtaining data through the Internet, like phishing e-mails.
   5. Large scale theft of data or data breaches is carried out for large scale fraud.

C. Laws Responding to Identity Theft
   1. Health Insurance Portability & Accountability Act (HIPAA)
   2. Federal Identity Theft Assumption and Deterrence Act of 1998
   3. Gramm-Leach-Bliley Act of 1999
   4. Health Information Technology for Economic and Clinical Health (HITECH) Act
   5. Texas Business and Commerce Code (Title 11, Chapter 521, Section 521.053)
   6. Texas Government Code (Title 10, Chapter 2054, Section 2054.1125)
   7. OMB Memorandum M-07-16

D. Mitigating Risks
   1. Administrative Risks
      a. The framework of administrative risks include security management and personnel; information access; workforce training and management; and evaluation.
   2. Physical Risks

    a. The framework of physical risks includes facility access; transfer, disposal, and re-use of electronic data; electronic encryption.
    b. Physical risks are the easiest of the risks for an organization to control.
3. Technical Risks
    a. The framework of technical risks includes authorized access to data; audit controls; improper alteration or destruction of data; and transmission security.

E. 10 Privacy Framework Questions You Should Ask (Source: GTAG 5)
1. What privacy laws and regulations impact the organization?
2. What type of personal information does the organization collect?
3. Does the organization have privacy policies and procedures with respect to collection, use, retention, destruction, and disclosure of personal information?
4. Does the organization have responsibility and accountability assigned for managing a privacy program?
5. Does the organization know where all personal information is stored?
6. How is personal information protected?
7. Is any personal information collected by the organization disclosed to third parties?
8. Are employees properly trained in handling privacy issues and concerns?
9. Does the organization have adequate resources to develop, implement, and maintain an effective privacy program?
10. Does the organization complete a periodic assessment to ensure that privacy policies and procedures are being followed?