MAULDIN & JENKINS

300 Mulberry Street
Suite 300
Macon, GA 31201
www.mjcpa.com
478.464.8000
800.277.0050

Our Resources

As always, we are available as a resource to you as questions arise.

Please contact any of our governmental partners and managers, at 1-800-277-0050 for assistance.

Miller Edwards	medwards@mjcpa.com
Meredith Lipson	mlipson@mjcpa.com
Joel Black	jmblack@mjcpa.com
Wade Sansbury	wsansbury@mjcpa.com
Alison Wester	awester@mjcpa.com
Adam Fraley	afraley@mjcpa.com
Doug Moses	dmoses@mjcpa.com
Matt Hill	mhill@mjcpa.com
James Bence	jbence@mjcpa.com
David Irwin	dirwin@mjcpa.com
Craig Moye	cmoye@mjcpa.com

You may subscribe to receive Mauldin & Jenkins Governmental Accounting News, by emailing Sydney Stewart at sstewart@mjcpa.com or by calling 770-955-8600.

MAULDIN & JENKINS

Governmental Accounting News

Cybersecurity Awareness

By Alison Wester

Cybersecurity breaches have become more and more common in the public and private sector. Home Depot, Target, Anthem and the IRS have been victimized by hackers. These incidents have made headlines and many Americans received notices offering credit monitoring or other services in response. On February 13, 2015, the President signed an Executive Order in Silicon Valley to create a collaboration of Information Sharing and Analysis Organizations (ISAOs) to facilitate the sharing of cyber-attack information across the public and private sector. The expectation is that the ISAOs would be organized along common grounds including sector, industry or geography to name a few. At the same time, the Administration added the Cyber-Threat Intelligence Integration Center to the Department of Homeland Security. Michael Daniel, White House cybersecurity coordinator, says this is the government getting its wiring straight.

State and local governments should also "get their wiring straight" and consider their information technology infrastructure and how their constituents, employees and those charged with governance interact with them. Network configurations, wireless access, the connection of external devices and Virtual Private Networks (VPN) all create points of entry for a possible cyber-attack. Much like a natural disaster, a cyber-attack could create a serious issue and operational interruption.

According to Randy Upchurch, CISA, CISSP and the Director of Information Technology services at Mauldin & Jenkins, "The hot topic now in power and utilities is SCADA. Amazingly, Chattanooga is a leader in security research of SCADA systems." These Supervisory Control and Data Acquisition systems (SCADA) are used in a variety of ways within a governmental entity. They open/close switches, regulate pressure, turn electrical systems on/off and regulate chlorine distribution. SCADA systems control functions in all sorts of power plants, factories, water facilities, nuclear reactors and prisons to name a few. For state and local governments, attacks that might allow hackers to remotely control key parts of the operations at essential facilities are a big concern.

The following steps can aid in gaining an understanding of the risks associated with your government's information technology infrastructure and allow an entity to mitigate those risks.

- Review your inherent risks, overall network configuration and disaster recovery plan.
- Discuss cybersecurity concerns, objectives at appropriate levels within the governmental entity.
- Understand how cybersecurity awareness is communicated to employees.
- Document your information technology controls and procedures to protect against and respond to a potential threat.

External consultants can assist a governmental entity in these evaluations while providing professional advice and guidance on best practices. Please contact Mauldin & Jenkins if we can be of assistance to you.

Rotating or Not Rotating Auditors

By Miller Edwards

There are proponents in the governmental sector that believe in changing auditors periodically. The belief is that changing auditors improves the quality of an audit by providing a "fresh look".

This issue was addressed in the following article posted on the AICPA's Center for Audit Quality website in July of 2015:

> ***Accounting Today*** reports that a new academic paper calls mandatory audit firm rotation into question. Based on a complex experiment involving students who did not even know they were playing the role of auditors, **the study concludes that mandatory rotation could inhibit professional skepticism rather than encourage skepticism**.
>
> "**Professional skepticism requirements are intended to elevate auditors' skepticism of their clients and, ultimately, audit quality**," the study says. "**This benefit disappears and even reverses when auditors rotate**. That is, rotation and a skeptical mindset interact to the detriment of audit effort and financial reporting quality."
>
> The study argues that auditors who are subject every few years to mandatory rotation feel less confident about their ability to audit a new client. "Rotating auditors, aware that they will not be in a long-term relationship, will...likely perceive themselves to be less competent in evaluating the honesty or dishonesty of the [corporate] manager relative to auditors who do not rotate." As a result, "**rotating auditors would find it difficult to garner psychological support for the probability of manager dishonesty, leading them to be less likely to choose high levels of audit effort than non-rotating auditors**."

The above conceptual thoughts as researched and issued by ***Accounting Today*** and the AICPA Audit Quality Center are considered to be relevant to all certified public accounting firms. We tend to agree with the thoughts communicated herein by the AICPA's Center for Audit Quality. That being said, if you feel differently from the conceptual thoughts communicated above, and that a rotation of auditors is necessary, it is important to note that Mauldin & Jenkins has substantial people resources, and can accommodate a change in: 1) lead partner, 2) quality assurance partner, 3) audit staff, and 4) office, should your government believe such changes are necessary.

New OPEB Standards

By: Tim Lyons

In a move that was widely expected to come after the Governmental Accounting Standards Board (GASB) issued the new pension standards in June of 2012, the GASB issued Statement No. 74 *Financial Reporting for Postemployment Benefit Plans Other Than Pension Plans* and Statement No. 75 *Accounting and Financial Reporting for Postemployment Benefits Other Than Pensions* in June of 2015. These new standards will significantly change the accounting and financial reporting related to other postemployment benefits (OPEB) plans offered by governments to its employees and retirees.

"These OPEB standards usher in the same fundamental improvements in accounting and financial reporting that were previously introduced for pensions," said GASB Chairman David A. Vaudt, in a news release dated June 2, 2015. "Because OPEB promises represent a very significant liability for many state and local governments, it is critical that taxpayers, policy makers, bond analysts, and others are equipped with enhanced information, which will enable them to better assess the related financial obligations and annual costs of providing OPEB," said Chairman Vaudt.

As noted by the GASB, these new standards essentially mirror Statements No. 67 and 68 issued for pension plans. Plan sponsors will be required to record a net OPEB liability in a statement of net position as well as a portion of the net OPEB liability for those sponsors who participate in cost-sharing plans. Statement No. 74, which replaces Statement No. 43, addresses reporting by OPEB plans that administer benefits on behalf of governments and is effective beginning with fiscal years ending June 30, 2017. Statement No. 75, which replaces Statement No. 45, addresses reporting by governments that provide OPEB to their employees and for governments that finance OPEB for employees of other governments and is effective beginning with fiscal years ending June 30, 2018.

www.mjcpa.com