

AGENDA

Joint Administrative Services Board

April 22, 2013 1:00 p.m.

Joint Government Center

1. **Call to Order.**
2. **Approval of Minutes. (February 25 Minutes Attached pg. 2).**
3. **Update from Director.** Four *credit cards* have been cancelled and reissued due to fraudulent activity from culprits outside Clarke County. *Travel Policy* issues: per diem payments for meals with no receipts vs. daily limits with receipts; restrictions on mileage reimbursements; valet parking; missing detailed receipts; variable reporting of mileage.
4. **ERP Implementation Guideline.** Please find attached a generalized outline of actions needed to implement the ERP system. (p. 10)
5. **ERP Research Documents:**
 - a. GFOA/Microsoft Study on ERP in the Public Sector.
 - b. GFOA Consulting Proposal.
 - c. Economics of the Cloud for the Public Sector.
 - d. Gartner on Cloud Security. (p. 11)

3. Update from Director

Joint Technology Plan adopted by Supervisors and School Board. Funding for training and study of Fiber Backbone included in budget requests. Health Insurance deductible creep.

Tom Judge advised that the Joint Technology Plan had been approved without change by the Supervisors and the School Board. The Plan includes ERP and the fiber backbone study.

Mr. Judge provided an historical overview of increases in health insurance premiums, as well as changes in offered plans.

4. Fraud Tip Line Update

Archana McLaughlin, County Attorney, will discuss her findings into the confidentiality of information provided through a fraud tip line.

Archana McLoughlin, County Attorney, joined the Board to provide legal guidance in the consideration of the establishment of a fraud and abuse hotline. She summarized her memorandum titled *Fraud and Abuse Hotline*, which she distributed with examples of fraud programs from Prince George and Hanover Counties.

Fraud and Abuse Hotline

Confidentiality and Freedom of Information Act (FOIA)

- Any reports made to the hotline would be public records because the JAS is a public body under FOIA. Pursuant to FOIA public records are generally made available to the public when requested.
- There are, however, exceptions for certain investigative records. The exemptions are qualified and apply only while the investigation is active.

See below the relevant excerpt from Virginia Code § 2.2-3705.3(7) that lists exclusions from FOIA disclosure requirements:

"Investigative notes, correspondence and information furnished in confidence, and records otherwise exempted by this chapter or any Virginia statute, provided to or produced by or for (i) the Auditor of Public Accounts; (ii) the Joint Legislative Audit and Review Commission; (iii) an appropriate [federal or state] authority as defined in ~~§ 2.2-3010~~ with respect to an allegation of wrongdoing or abuse under the Fraud and Abuse Whistle Blower Protection Act (~~§ 2.2-3009 et seq.~~); (iv) the Office of the State Inspector General with respect to an investigation initiated through the State Employee Fraud, Waste and Abuse Hotline or an investigation initiated pursuant to Chapter 3.2 (~~§ 2.2-307 et seq.~~); (v) the committee or the auditor with respect to an investigation or audit conducted pursuant to ~~§ 15.2-825~~ [urban county executive form of government]; or (vi) the auditors, appointed by the local governing body of any county, city or town or a school board, who by charter, ordinance, or statute

have responsibility for conducting an investigation of any officer, department or program of such body."

- The records created under these circumstances would be confidential while being investigated. Once the investigation is closed FOIA does require disclosure as described in the statute.

See below excerpt from Virginia Code § 2.2-3705.3(7)

"Records of completed investigations shall be disclosed in a form that does not reveal the identity of the complainants or persons supplying information to investigators. Unless disclosure is prohibited by this section, the records disclosed shall include, but not be limited to, the agency involved, the identity of the person who is the subject of the complaint, the nature of the complaint, and the actions taken to resolve the complaint. If an investigation does not lead to corrective action, the identity of the person who is the subject of the complaint may be released only with the consent of the subject person. Local governing bodies shall adopt guidelines to govern the disclosure required by this subdivision."

Implementation

- Do JAS records qualify for the exemption under the statute?
 - Is there any evidence that the JAS "by charter, ordinance, or statute have responsibility for conducting an investigation of any officer, department or program of [the County Board of Supervisors]?"
 - If a record of an active investigation is the subject of a FOIA request, and we would likely want to rely on this section, so we must determine whether this body fits, and if not, what we can do to make it fit.
 - Also exceptions for criminal investigation files. Va. Code §2.2-3706
- See below excerpt from Virginia Code § 15.2-2511.2(B). Duties of local government auditors.

Any fraud, waste, and abuse auditor appointed by the local governing body of any county, city, or town having a population of at least 10,000, or any town constituting a separate school division regardless of its population, who by charter, ordinance, or statute has responsibility for conducting an investigation of any officer, department or program of such body, shall be responsible for administering a telephone hotline, and a website, if cost-effective, through which employees and residents of the locality may report anonymously any incidence of fraud, waste, or abuse committed by any such officer, or within any such department or program, of that body. Such auditor may inform employees of the locality of the hotline and website, if any, and the conditions of anonymity, through the conspicuous posting of announcements in the locality's personnel newsletters, articles in local newspapers issued daily or regularly at average intervals, hotline posters on local employee bulletin boards, periodic messages on local employee payroll check stubs, or other reasonable efforts.

- Board must develop and adopt guidelines that "govern the disclosure required by th[e] subdivision."
- As a practical matter, you can not disclose information that you never had
 - One way to keep it anonymous is to establish a telephone hotline with caller ID and call back features disabled.
 - Open up line to public, not just employees.

Discussion followed after the summary; the Board concurred on the following:

- A hotline may not be the best course of action but does warrant further consideration.
- Review current complaint investigation process to determine if there is more that can be done. *It was noted that many complaints are about situations over which the County has no control and/or jurisdiction.*
- Further discussion is needed to determine the value.
 - Reporting quality could present issues and limit the ability to conduct a proper investigation.
 - Resources are limited and subsequent investigations could be time consuming.
- Establish definitions, such as Hanover County's, and train employees on fraud, waste and abuse.
- Considerations if implemented:
 - Create a form for staff use that specifically asks the question as to whether the caller wishes to remain confidential.
 - Set up the reporting system to protect anonymity.
 - Forward complaints to the appropriate agency for investigation.
 - Identify resources to pursue investigations.
 - Establish a timeframe for reporting and start of investigation.
 - Establish thresholds.
- Tom Judge, with Archana McLoughlin, will further research the matter including follow up with County IT to determine if a section could be added to the County's website that would include definitions for fraud, waste and abuse and where to report.

5. Health Insurance Renewal

Please find the health insurance renewal information attached. This requires the consideration and approval of the Board. The rate increases 7%, but there are no changes to the terms of the agreement. However, Anthem has substituted some underlying vendors for others (mental health, pharmacy, dental, and vision).

Tom Judge advised that there were no changes in plan terms however there were changes in underlying vendors: Anthem will move in house mental health, pharmacy, dental and vision coverage; Delta will be the dental vendor for the high-deductible plan.

Following brief discussion, Mike Hobert, seconded by David Ash, moved to recommend adoption of the Anthem renewal as proposed to the respective bodies. The motion carried as follows:

- David Ash - Aye
- J. Michael Hobert - Aye
- Sharon Keeler - Absent
- Michael Murphy - Aye
- Charles "Chip" Schutte - Aye

FY 14 Monthly Health Benefit Rates		Effective 7/1/2013			
Source: Joint Administrative Services					
A. Plan Rates	Cost	Employer	Employee	Employer FY 14 Share	Employer FY 13 Share
KA 250 Plan Option					
<i>Regular Full Time</i>					
Single	536.00	456.65	79.35	85%	85%
Dual	992.00	498.02	493.98	50%	50%
Family	1,447.00	727.34	719.66	50%	50%
<i>Transportation, Food Service & Other</i>					
Single	536.00	385.31	150.69	72%	72%
Dual	992.00	420.22	571.78	42%	42%
Family	1,447.00	613.72	833.28	42%	42%
KA 500 Plan Option					
<i>Regular Full Time</i>					
Single	487.00	458.65	40.35	92%	92%
Dual	919.00	498.02	420.98	64%	64%
Family	1,342.00	727.34	614.66	54%	54%
<i>Transportation, Food Service & Other</i>					
Single	487.00	385.31	111.69	78%	78%
Dual	919.00	420.22	498.78	46%	46%
Family	1,342.00	613.72	728.28	46%	46%
TLC High Deductible					
<i>Regular Full Time</i>					
Single	409.00	409.00	.00	100%	100%
Dual	757.00	485.25	271.75	61%	61%
Family	1,104.00	677.56	426.44	61%	61%
<i>Transportation, Food Service & Other</i>					
Single	409.00	345.11	63.89	84%	84%
Dual	757.00	392.57	364.43	52%	52%
Family	1,104.00	571.71	532.28	52%	52%
B. Account Contributions					
<i>Regular Full Time</i>					
TLC Health Savings Account Contribution (single)		47.65			
TLC Health Savings Account Contribution (dual)		32.77			
TLC Health Savings Account Contribution (family)		49.79			
<i>Transportation, Food Service & Other</i>					
TLC Health Savings Account Contribution (single)		40.29			
TLC Health Savings Account Contribution (dual)		27.65			
TLC Health Savings Account Contribution (family)		42.01			
C. Total Employer Cost Per Group Health Member					
<i>Regular Full Time</i>					
Single Health		458.65			
Dual Health		498.02			
Family Health		727.34			
TLC Single Health & "HSA"		458.65			
TLC Dual Health & "HSA"		498.02			
TLC Family Health & "HSA"		727.34			
<i>Transportation & Food Service</i>					
Single Health		385.31			
Dual Health		420.22			
Family Health		613.72			
TLC Single Health & "HSA"		385.31			
TLC Dual Health & "HSA"		420.22			
TLC Family Health & "HSA"		613.72			

Note: Where two employees are married, and they together opt for either a dual or family option, the employer will pay two times the single employer contribution for the plan option selected.

METHOD:
 Force TLC employee single contribution to zero.
 Proportion other rates to percentage contributions from prior year.
 Force 250 employer contribution to same as 500 contribution.
 Force "HSA" contribution so total employer equal across plans.

6. Affordable Care Act Issues

Please find documents attached from Anthem outlining the rollout of the A CA. We are receiving regular correspondence from various sources warning of the need to adjust policies, etc. These include how part-time employees are to be defined, whether employees are free to purchase their insurance from health insurance exchanges, notification requirements, automatic enrollment, etc.

Tom Judge advised that he had been researching the matter to determine the impacts. Highlights include:

- Anthem provided the "Navigating the next phase of health care" brochure included in the meeting packet.
- JV Arthur and BB&T are providing information to clients.
- Regulations are being rewritten.
- 30-hour employee calculation may affect Parks and Recreation staff, part-time school employees, long-term substitutes, etc.
- Employees will be automatically enrolled and it will be the employee's responsibility to reject.
- The new plan takes effect January 1, 2014.

Miscellaneous

Tom Judge distributed and summarized the article below.

Automatic budget cuts in Virginia

By The Associated Press

The White House released lists for each state on Sunday of potential effects of automatic spending cuts set for Friday. The White House compiled the numbers from federal agencies and its own budget office. The numbers are based only on the \$85 billion in cuts for this fiscal year, from March- September, that are set to take effect Friday. As to whether states could move money around to cover shortfalls, the White House said that depends on state budget structures and the specific programs. The White House did not have a list of which states or programs might have flexibility. The White House says the cuts that could affect Virginia include:

Military

About 90,000 civilian Department of Defense employees in Virginia would be furloughed. Funding for Army base operations would be cut by about \$146 million. Air Force operations funding would be cut by about \$8 million. Maintenance of 11 Navy ships in Norfolk would be canceled and four projects at Norfolk, Dahlgren and Oceana would be deferred. Other modernization and demolition projects would be delayed.

Teachers and schools

Virginia would lose about \$14 million in funding for primary and secondary schools. About 190 teacher and aide jobs would be at risk. Virginia also would lose about \$13.9 million in funding for about 170 teachers, aides, and staff who help children with disabilities.

Public health

Virginia would lose about \$2.1 million in funding to help prevent and treat substance abuse. The state also would lose about \$764,000 in funding to help improve its response to infectious diseases, natural disasters, and other public health threats. A \$337,000 cut in funding for the Virginia State Department of Health would reduce the number of HIV tests by around 8,400. Virginia also would lose about \$241,000 for vaccinations for children, including measles, mumps, rubella, tetanus, whooping cough, influenza, and Hepatitis B.

Environment

Virginia would lose nearly \$3 million in funding for clean water, air quality and prevention of pollution from pesticides and hazardous waste. The state also would lose \$826,000 for fish and wildlife protection.

Head Start

About 1,000 children in Virginia would lose Head Start and Early Head Start services.

Work-study

Aid would be provided to around 2,120 fewer low income students in Virginia to help them finance the costs of college. Funding for workstudy jobs would go to around 840 fewer students.

Law enforcement and public safety

Virginia would lose about \$276,000 in grants for law enforcement, prosecution and courts, crime prevention and education, corrections and community corrections, drug treatment and enforcement, and crime victim and witness initiatives.

Job search assistance

Virginia would lose about \$348,000 in funding for job search assistance, referral, and placement. About 18,390 people would be affected.

Domestic violence

Virginia could lose up to \$172,000 in funding for services to victims of domestic violence.

Seniors

Virginia would lose about \$1.2 million in funding to provide meals for seniors.

Next Meeting

The next regularly scheduled meeting of the Joint Administrative Services Board is Monday, March 18, 2013 at 1:00 pm in Meeting Room AB at the Berryville Clarke County Government Center.

Adjournment

At 2:34 pm, hearing no objection, Chairman Schutte, adjourned the meeting.

Minutes Recorded and Transcribed by Lora B. Walburn

ERP Implementation Guideline

- I. Communicate decision to affected employees. Clarification of business practices.

- II. Establish Team.
 - a. Determine local Project Manager.
 - b. Identify knowledgeable citizens for guidance.
 - c. Build on previous focus groups to develop specialized expertise by function.
 - d. Clarify roles of Boards, IT directors, Department heads, focus groups. Verify cooperation of semi-independent agencies.
 - e. Seek sources of assistance from: VITA, Shenandoah University Institutional Computing, similarly situated communities (Portsmouth, Prince George, Staunton, and Alexandria), Center for Innovative Technology, etc.
 - f. Evaluate whether we have identified the expertise to carry out the project, or whether a consultant should be hired to guide it.

- III. Establish Requirements.
 - a. Detail specifications for each module.
 - b. Cloud versus Server.
 - c. Data Standards and Data Independence (lock-in avoidance).
 - d. Best Practices.
 - e. Phase-in versus Big Bang.
 - f. Timing vis-à-vis tax year and fiscal year.
 - g. Historical data vs. point forward.
 - h. Web based.
 - i. Disaster Recovery and Security.
 - j. Web Training vs. Travel Training.
 - k. Ability to interface with Rec-Trac, Café Enterprise, ESRI, Southern Software, etc.

- IV. Issue a Request for Proposals.
 - a. List of Potential Vendors (Tyler, Sungard, New World, Microsoft Dynamics, OpenRDA, Edmunds, etc.)
 - b. Demonstrations and site visits.
 - c. Evaluation Criteria.
 - d. JAS Board to evaluate.
 - e. Financial Data and long range corporate commitment.
 - f. Proceed to contract.

- V. Develop Implementation Plan.

Sponsored by:

NETWORKWORLD

This story appeared on Network World at

<http://www.networkworld.com/news/2013/041013-gartner-cloud-security-268587.html>

News

Gartner: Long hard climb to high level of cloud computing security

Gartner analyst Jay Heiser says Gartner clients often "disappointed" by what they see offered as security and reliability provisions in cloud contracts

By Ellen Messmer, Network World
April 10, 2013 12:24 PM ET

Network World - It's still a long, hard climb to get to a high level of security in cloud computing, according to Gartner research vice president Jay Heiser, who said business and government organizations with sensitive data appear likely to hold back from cloud-based services until things improve.

Sponsored by:

"Finance tends to be more conservative about cloud computing than small business," said Heiser in his online presentation to Gartner clientele yesterday. In "Prepare for and Minimize the Security Risk of Cloud Computing," Heiser expressed the view that it's somewhat simpler to establish a security baseline when using infrastructure-as-service (IaaS) than it is for software-as-service (SaaS) if only because there's more flexibility and

less dependence on the competence of the service provider. But overall, cloud service providers aren't as clear as they should be concerning matters such as their business continuity and disaster-recovery practices, making it hard to win customer confidence.

[RELATED: Gartner: 10 critical IT trends for the next five years]

[BACKGROUND: Evolving security standards a challenge for cloud computing, expert says]

"Gartner clients are almost universally disappointed" by what they regard as the incompleteness in cloud-computing contracts where they still don't see the level of specificity related to security they expect, said Heiser. "Cloud contracts are incomplete," he emphasized.

The struggle to define both technologies and legal obligations between the cloud and the customer is a topic that has been taken up by both the federal government in its FedRAMP program that seeks to certify cloud-service providers for government use, and the organization Cloud Security Alliance (CSA), which has several working groups pouring enormous effort into defining industry standards.

Heiser also pointed out that the American Institute of Certified Public Accountants (AICPA) has replaced its SAS70 certification with what's service provider certification called with SOC 1, and there's now a SOC 2 and SOC 3 as well to indicate service provider systems trust and security.

But while applauding all of these standardization efforts for security in cloud computing as significant, Heiser said FedRAMP, which is supposed to be operational next year, and the CSA standards are still early projects and their impact may be years away. Heiser had similar sentiments about the ISO/IEC 27017 cloud security standard and the 27018 cloud privacy standard. All of these cloud-computing security efforts are worthwhile but they will take somewhere between a year to five years to be considered mature, he says.

In the meantime, businesses and government have to pin down their requirements and evaluate potential cloud services and their security options as well as they can. The starting point should be looking at the sensitivity of the data going into the service, Heiser says. Companies have to ask questions such as what kind of impact would be the loss of it be, is it of critical competitive value, and is the data subject to regulatory concerns. "It comes down to determining the appropriateness of the service," he says.

The most mature and readily available security controls today in cloud computing are associated with identity and access management mechanisms and server-based encryption, he said. But cloud customers have to ask how encryption keys are managed and stored and if the risk is acceptable, he noted. Gateway-based encryption, or what's sometimes called a broker gateway or proxy, is another option, and it's changing quickly, he added. Forensics investigations are not really viable today, he noted, and in terms of overall security controls, it will probably take five to 10 years to really see a "solid set of technologies" for cloud computing.

The economic appeal of cloud computing is strong and sometimes it does appear economic benefits outweigh potential risks. Gartner is advising clients in general to allow low-sensitivity data to be considered for cloud services; but if it falls in the "medium" range of sensitivity, there's a strong need to conduct a risk assessment. And if the data is of high sensitivity, it should not be considered feasible or permissible for cloud services.

This process also means making sure that the business managers are engaged and realize they "own" the data, and are up to speed on the risks associated with cloud computing, says Heiser.

Nonetheless, cloud services providers rarely offer any indemnification against hacking, Heiser says. And SaaS remains more "mysterious" than IaaS in terms of making it clear how they really operate even as customers basically enter into a kind of supply chain cloud. Since one risk is that a cloud provider might go out of business, there needs to be assurance that the provider can return data or has a contingency plan for back-up. When the Mumboe SaaS went out of business two years ago, they gave customers two weeks to go get their data back, mentioned Heiser. That was a wake-up call of sorts that clouds sometimes do evaporate, and plans need to be made for these kind of downpours.

Even at some of the household names in cloud-computing today — Amazon, Google, Microsoft — there have been instances where data has disappeared, at least for a time, or never returned, says Heiser. "Restoration is not an easy process," he adds. "Put loss of service and availability at the top of your list." Live upgrades of services can lead to widespread data corruption, he pointed out.

IT managers have become accustomed to the idea they have control over what they can do in-house in terms of the application, services, servers, storage and network, and security. He says they need to fully realize that this accustomed level of flexibility isn't going to be there in cloud computing by its very nature.

Ellen Messmer is senior editor at Network World, an IDG publication and website, where she covers news and technology trends related to information security. Twitter: MessmerE. E-mail: emessmer@nww.com.

Read more about security in Network World's Security section.

All contents copyright 1995-2013 Network World, Inc. <http://www.networkworld.com>