COUNTY OF MILWAUKEE
INTEROFFICE COMMUNICATION

Date : June 1, 2012

To : Supervisor Willie Johnson Jr., Chair, Finance and Audit Committee

From : Chris Lindberg, Chief Information Office & Director of Information Management Systems Division

Subject: Informational Report: Open Source Software Study

2012 BUDGET REQUEST

"IMSD shall prepare a report including a cost benefit analysis of converting the currently deployed web, calendar, and email servers to an open source software platform. Open source software is commercial-grade software that is built through a peer-review process. It is usually much less expensive than traditional commercial software and, based on studies, more secure. Open source applications, including email, calendar and collaboration, have already been deployed at institutions such as the U.S. Department of Defense and UW-Milwaukee."

REPORT OBJECTIVES

The primary objective of the open source study is to determine if cost savings can be generated for Milwaukee County government through the adoption of open source software. A secondary objective is to determine if open source software is more secure than commercial software.

SUMMARY OF FINDINGS

1. *Cost Savings:* Open source software will not save Milwaukee County money. Instead, it will require significant additional investments in time and dollars that will detract IMSD from its primary missions of supporting the businesses of Milwaukee County and strengthening security in support of HIPAA and CJIS requirements.
2. *Security:* Both commercial and open source software can be appropriately secured provided mandatory investments in support and maintenance are made in either environment.

IMSD DEPARTMENTAL DESCRIPTION

The Milwaukee County Information Management Services Division (IMSD) provides information technology services and support to over 43 County departments and divisions.

Further breakdown includes the servicing, support and management of:

- ~143 major applications (e.g., G/L, email, CJIS, document management) executing on Mainframe Z/OS and Windows Server 2003/2008 on VMWare hosts in a Milwaukee County data center
- ~3500 desktop computers executing Windows XP and a variety of applications
- Email and calendaring for all employees via Lotus Notes

- Wide and local area networking across Milwaukee County connecting all facilities
- Secure Internet access for all facilities and employees
- Help Desk Service and Support for all employees and all applications
- Information and access security
- Business continuity and disaster recovery
- Telecommunications
- Public Safety Radio system
- Mail Room

The current staffing level for IMSD includes 61.5 internal positions of which 20% are currently vacant.

RESULTS OF OPEN SOURCE STUDY: SUPPORTING INFORMATION

COST FINDINGS

Scenarios

- *Scenario #1:* Microsoft continues to be the primary application, operating system and backend services provider hosted on VMWare Virtual Servers. The Microsoft Enterprise Agreement Program is leveraged not only for Windows 7 desktop and all backend services but also for full email, calendaring, collaborative and web services.

- *Scenario #2:* To ensure technical landscape simplicity as a means to generate cost savings, all systems (servers, applications and databases) are converted to open source software. Staffing (model, people, talent and job descriptions) is appropriately altered to support the new environment in a secure fashion.

- *Scenario #3:* Secure open source systems are installed to provide email, calendaring, limited collaborative services and web access services only. Applications are remediated for execution on open source web and application servers. All other applications and services remain the same. As in Scenario #2, staffing (model, people, talent and job descriptions) is appropriately altered to support the new environment in a secure fashion The environment is managed for security.

Common Planning Assumptions:

- All email, calendaring and collaborative services (commercial and open source) are provided via commercial “cloud-based” services
- The Microsoft Enterprise Agreement Program is leveraged fully and appropriately for Scenarios #1 and #3
- All other open source systems (e.g., database, application servers and web servers) are assumed to be “free”
- Health Insurance Portability and Accountability Act (HIPAA) and Criminal Justice Information System (CJIS) security compliance assured through

  - Commercial Software: Vendor code management and patching
  - Commercial Open Source: Vendor code management
  - Cloud-based services: HIPAA Business Associate Certificates
  - Full "free" Open Source: In-house code review and management
- Current Mainframe G/L and CJIS systems remain in place

3 Year Cost Estimates

	Scenario 1	**Scenario 2**	**Scenario 3**
Software Licensing - Microsoft - Zimbra	$1.9 M	$1.0 M $2.1 M	$1.0 M $2.1 M
Email and calendaring implementation Costs	Same[1]	Same[1]	Same[1]
Application Remediation or Replacement	$0.2	$3-5 M	$2-4 M
Platform elimination savings	$0.14 M	$0.14 M	$0.14 M
Staffing Changes	No changes	+6 FTEs $2.5 M fully loaded	+3 FTEs $1.3 fully loaded
3-Year Estimated Costs	$2.0 M	$8.5–10.5 M	$6.3-$9.5 M

[1] Implementation costs for each scenario are not differentiators and as such are not included in the 3-Year Estimated Cost analyses. These costs are in addition to those stated.

SECURITY ANALYSIS

Microsoft, Apple, SUN and other commercial software manufacturers manage their proprietary code and provide software "patches" that correct deficiencies in security and provide other enhancements as well. Organizations using commercial software products must ensure that software remains up-to-date through a managed "patching" process. In most cases, automated tools are provided that install and configure patches.

Commercial providers of open source systems (e.g., Zimbra by VMWare) monitor and manage software code much like manufacturers of proprietary code as described above. These services are provided at a cost that is captured in their commercial licensing fees.

The security management of true open source software systems and code requires the implementation of in-house code review, testing and implementation processes. These processes require specific skills (sourced internally or externally) across the major platforms (application, database and web server). As a result, the staffing model would have to be altered to accommodate these important functions.

HIPAA compliance is provided either directly from the commercial provider of software or cloud-based services, or must occur through the implementation of support processes and methods (code review and testing). These processes require specific skills.

OTHER FACTORS TO CONSIDER

- **Licensing:** Commercial software licensing is transactional in nature. The software and/or its functions can be distributed outside the organization once licensing terms are met and the financial transaction is completed. Open source licensing grants the user the ability to execute the software but not necessarily the right to redistribute it or its functions to other parties outside the organization. This is a gray legal area for open source software. Should Milwaukee County government become a service provider to other municipalities, extension of licensing could be an issue
- **"Owning" the Code:** An attractive feature of open source software is that the code is freely available for modification and customization. This is not the case for commercial software where code is tightly controlled and managed by the manufacturer. The key question for Milwaukee County and its base of technology is simple: Should IMSD customize code for use in County government or seek commercial solutions that meet 80-90% of the business requirements? Customization has significant costs that would have a direct impact on budget, projects and schedules. Best practices strongly suggest that organizations not customize software unless a strong business case supports the outyear costs.
- **Software is continually improving:** A central thesis to the advantage of open source software is that a world community is constantly striving to add features and benefits to open source systems. This is fundamentally true. However, the same is also true for commercial providers of software. Failure to adapt generally means failure to sell and failure to thrive. Established commercial software manufacturers remain established because they adapt and continually improve their offerings.
- **Company stability:** Open source software doesn't "go out of business" when economic times are bad or markets change. The same is not true for commercial software developers. Failure to adapt general results in business failure. Unless business requirements are highly specialized requiring acquisition of specialized software or extensive software customization, organizations should invest in the larger, stable commercial software . A great example of this is SAP, the premier provider of proprietary Enterprise Resource Planning software used by a large number of companies across the world.
- **Software stability and security:** All software, regardless of manufacturer (commercial or open source) occasionally suffers from stability or usability issues. Manufacturers and communities all continually develop corrections and enhancements to their software products.
- **Open does not mean free:** Many companies that adopt open source software because of the free licenses ignore the cost of installation, conversion, code maintenance, review and customization. These costs should be included in the total cost of ownership.
- **Code review and maintenance:** Open source software code review and maintenance should follow industry best practices and is the responsibility of the organization using the software. This has a cost in both terms of dollars and time.

- **Service levels:** Open source software providers do not provide guaranteed service levels. Problems are corrected when the open source community responds, and they are under no obligation to provide 24x7 service and support. Commercial software manufacturers do charge for support and maintenance but it comes with contractually guaranteed service levels. To mitigate the risk of system outages, organizations investing in open source solutions must invest in support services (external or internal).

  Supporting Notes:
  - *Accenture, a large and respected information technology consulting company requires service level contracts behind **commercially-provided** open source systems such as Zimbra.*
  - *The US Department of Defense requires the addition of in-house staff to support open systems software.*

RECOMMENDATION

IMSD's focus for the next several years will be the strengthening of information security compliance for Milwaukee County, and increasing the robustness and capabilities of IMSD and information technology within County government. Conversion of applications and underlying systems to open source software will be expensive, time consuming and distract the organization from fulfilling its primary mission.

The Chief Information Officer respectfully requests this report to be received and placed on file unless further action is required by the Committee.

Prepared By:

Chris Lindberg, IMSD
Chief Information Officer

cc: Chris Abele, County Executive
Amber Moreen, Chief of Staff, County Executive's Office
Marina Dimitrijevic, Chairwoman, County Board of Supervisors
Tia Torhorst, County Executive's Office
David Cullen, Vice Chair, Finance and Audit Committee
Patrick Farley, Director, DAS
Craig Kammholz,, Fiscal and Budget Manager, DAS
Steve Cady, Fiscal and Budget Analyst, County Board
Carol Mueller, Committee Clerk, Finance and Audit Committee
Laurie Panella, Deputy CIO, IMSD
Rich Foscato, Chief Solutions Officer. IMSD
Nick Wojciechowski, Chief Technology Officer, IMSD
Dan Laurila, Budget Analyst, DAS