

## **Tennessee Enterprise Communications Infrastructure – A Vision Becomes Reality**

### **EXECUTIVE SUMMARY**

The ability to communicate efficiently, effectively and securely is a necessary component of any government or business endeavor. State governments are no exception. This electronic communication has vastly changed the office environment. Today, electronic communication, through the network of approximately 40,000 PC's, provides this mission critical business function for the State of Tennessee government. A vision to provide an electronic communications infrastructure that seamlessly meets the needs of all State agencies is a strategic goal for the State of Tennessee. To provide this functionality within the State's government requires long-term vision, strong leadership, close integration and multi-agency cooperation.

There are several challenges that arise when designing an enterprise wide technology solution within state government. Those challenges range from pure technology to pure politics and can sometimes become impassable roadblocks. That is not the case within the State of Tennessee. By designing and implementing a solid technology solution with world-class service, support and well-defined policies and process those roadblocks seem to disappear and give way to economics and common sense.

The State of Tennessee has designed and implemented a solution that provides efficient, effective and secure messaging capability for all State agencies to utilize. The State's solution has a measurable hard dollar cost saving of more than \$24 million over a 6-year term. This is accomplished with a centralized management approach, the implementation of successful information security technologies and true government IT leadership.



## **Tennessee Enterprise Communications Infrastructure – A Vision Becomes Reality**

### ***Section A: Concise description of the business problem and solution, including length of time in operation***

The ability to communicate efficiently, effectively and securely is a necessary component of any government or business endeavor. Today most enterprise organizations primarily communicate through some form of an electronic interface, referred to herein as “messaging.” State governments are no exception. This electronic communication has vastly changed the office environment. Dictaphones, typewriters and secretaries who take shorthand are long forgotten. “Snail mail” has been relegated to primarily a mechanism for the delivery of periodicals and brochures. Today, electronic communication, through the network of approximately 40,000 PC’s, provides this mission critical business function for the State of Tennessee government. A vision to provide an electronic communications infrastructure that seamlessly meets the needs of all State agencies is a strategic goal for the State of Tennessee. To provide this functionality within State government requires long-term vision, strong leadership, close integration and multi-agency cooperation. The diversity of services and separate branches of government adds to what is already a unique challenge within the IT business world.

The following is a list of stakeholders with vested interest in the success of an enterprise messaging solution to address this need:

**Information Systems Council (ISC)** is the governing oversight authority for State technology and consists of eleven representatives from the legislative, executive, judicial branches and two private sector representatives.

**Office of the Budget, Department of Finance and Administration (F&A)**, is the central budget authority for State government.

**Office for Information Resources (OIR), F&A**, is the central technology authority for State government and the IT service provider to State agencies.

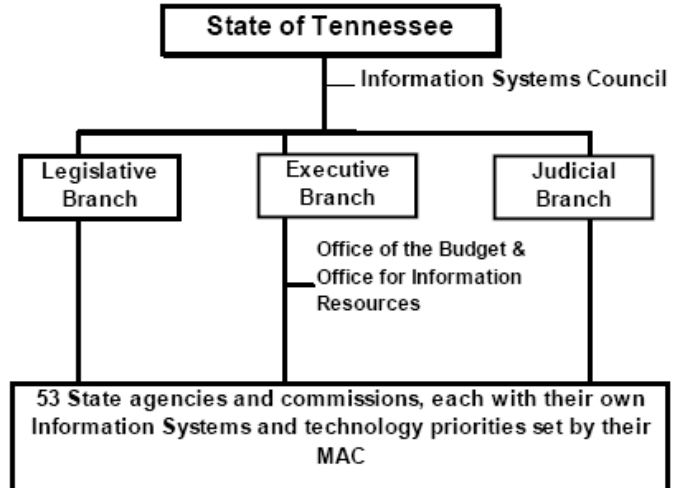
**The Citizens of the State of Tennessee**, or citizens who expect State government to produce efficient and successful technology solutions with their hard-earned tax dollars.

The problem:

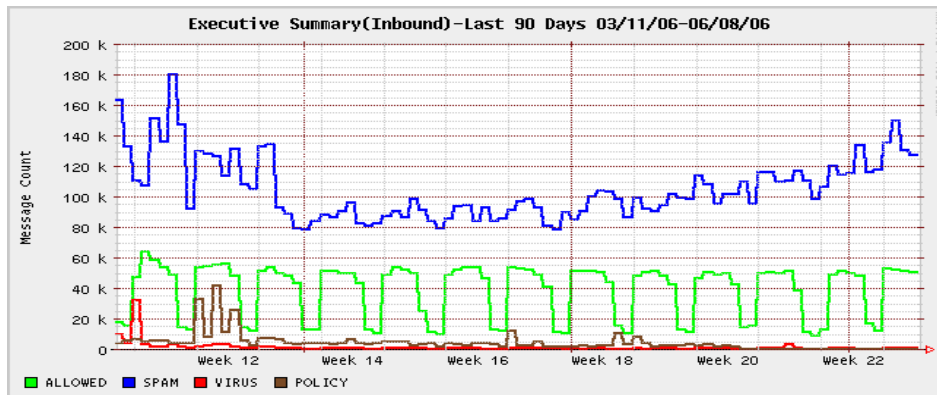
The primary problem with enterprise messaging services within state government is the complexity of providing a full-service, secure and economical messaging solution. Several issues contribute to this problem. First, the scope of the technology service is very large. There are approximately 39,500 employees within the State of Tennessee serving 53 separate agencies, across 3 branches of State government, which in turn serve approximately 6 million citizens. Second, the diversity and the split nature of State government agencies and management create an even more complex challenge.

State of Tennessee NASCIO Award Nomination 2006  
Enterprise Architecture

To the right: Diagram illustrating the distinct lines of separation and relationship of the stakeholders, OIR, and technology leadership within the State of Tennessee



Today, most of the State's employees are utilizing e-mail services and hundreds are utilizing instant messaging services. Electronic mail (e-mail) is the primary communication tool for business communication so the services are in high demand. We are seeing increased demand for secure instant messaging solutions. The solution currently provides that functionality internally. Second, federal funding sources allocated to individual agencies make it difficult to control IT projects toward a common goal. Establishing a common goal supported across the domains mentioned above is crucial to the success of a comprehensive service offering such as enterprise messaging. Finally, we can only be as strong as our weakest link, and when linking the messaging technologies all together across the State and all of the separate management domains and public offices, security poses a very large and complex challenge. In the *Symantec Internet Threat Report* covering the last half of 2005, Symantec states that one in 119 emails was determined to be a phishing attempt, up from one in 125. Symantec states that their products detected an average of 7.9 million phishing attempts per day, an increase of 39% over the first half of 2005. They also state that 'Spam' made up 50% of all monitored email traffic and that spam associated with financial goods and services was the most common type of spam, and lastly, that the United States was the country of origin of 56% of all spam. The following chart illustrates that same trend, with more significant and threatening numbers, when taking a look at the last 90 days of service within the State of Tennessee:

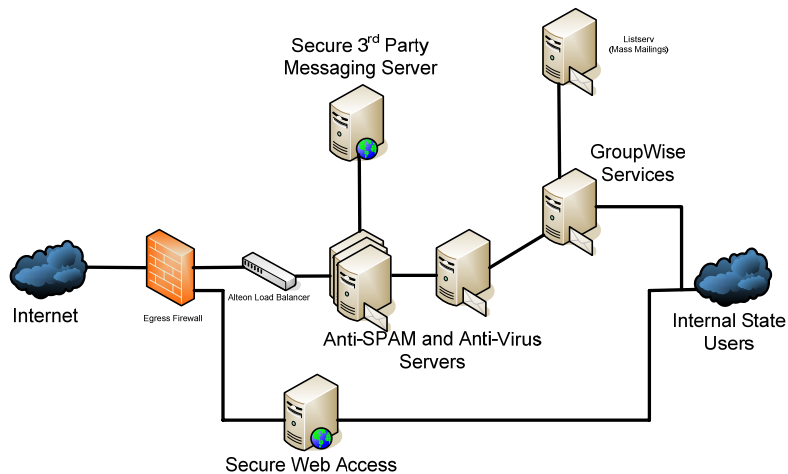


The number of spam messages being sent to recipients of the State is approximately 120,000 messages per day, or more than 60% of all messaging traffic. Messaging based malicious codes attacks (messages with viruses/worms attached) number in the thousands per day.

State of Tennessee NASCIO Award Nomination 2006  
Enterprise Architecture

The Solution:

The State of Tennessee has experience when solving complex technology problems. The Tennessee Information Infrastructure network and the State of Tennessee Information Systems Planning process are prime examples of that. The state followed suit with a suite of tools overlaid on the network to enable end users and State agencies to take advantage of electronic age messaging services. There are three major components of the solution, and when put together, the messaging package provides a compounded successful solution with multiple aspects. From a pure e-mail perspective the state's solution consists of a centralized core network of mail (SMTP gateways) servers coupled with distributed Novell GroupWise client/server software to push the services out to the end user. The services are centrally managed by the Office for Information Resources, a centralized technology and management office within the State of Tennessee. To deal with the security issues the State has implemented CipherTrust's Ironmail security technologies along with three separate anti-virus software technologies to deliver the e-mail service clean and secure.



There are 8 mail servers that function as the SMTP gateways for the environment. These are located in the state's data center. They in turn act as delivery mechanisms to the 71 post offices located throughout the state. The client access tool is GroupWise, which is distributed to all of the end users workstations. The solution also provides secure instant messaging services as well as web-based e-mail access for state workers without access to state managed computing assets.

Not only did the solution meet a very significant business requirement, it also enabled the State of Tennessee to provision the service efficiently and securely

Tennessee has been providing the centralized messaging service solution to agencies for several years. However, all of the various components were not active within the service for that entire amount of time. The implementation of a full service solution—centralized email, anti-Spam, secure Instant Messaging, and the ability to send email via the Internet securely, has been completed in 2006.

### ***Section B: Significance to the improvement of State Government***

This enterprise solution solves many issues and contributes to enhancements and security of groups within the State of Tennessee. The first of which is that it provides an efficient, low risk communication tool for State government. Low risk technology solutions offer stability of service and maintainability on a State's budget. By centralizing the messaging infrastructure the State realizes hard dollar savings in human resources, saving the State taxpayers hundreds of thousands of dollars per year. The solution is also able to significantly reduce the administrative effort required to analyze and address the spam issue. It increases employee productivity by reducing the time spent deciding if an e-mail is legitimate or spam and then disposing of the message if it is deemed to be spam. Second, and quite possibly the most significant improving factor is that the solution provides effective and efficient electronic communications statewide. Over 95% of all agencies, including all branches of State government, utilize this service and that number continues to grow. Typically, within governments a crippling factor to the success of enterprise wide solutions is the lack of participation across branches of government. Tennessee has provided an economical and efficient solution coupled with world-class support and process to make the service appealing for agencies in other branches of government. That factor alone has had a significant impact on the improvement of State government from an operational perspective. Finally, the solution helps the State foster due diligence in terms of regulatory compliance and legal liability. The State is able to limit legal liability by filtering out inappropriate content that may offend employees, or in some cases is against the law. The messaging solution provides the capability to deliver secure, confidential e-mail or instant messaging communications in accordance with laws and regulations such as the Health Insurance Portability and Accountability Act (HIPAA). Agencies are able to interact and communicate securely within the state agencies of Tennessee, as well as set up secure communications to third parties, including providing a secure communications channel to any of the 6 million State citizens, who fall outside the enterprise end user environment.

### ***Section C: Benefits realized by service recipients, taxpayers, agency or State***

There are several benefits provided as a result of the implementation of this service. To start, messaging centralization provides a capability to manage the messaging infrastructure with increased efficiency. The State provides this service to 39,500 employees with 3 FTEs. If the service were not centralized the State would need multiple FTEs wherever separate messaging environments were established. Centralization also provides the ability to control policy and design and implement new solutions efficiently. Without these contributing factors the State would need to spend millions of taxpayer's dollars on a dead end technology solution. This is critical to the success of any efficient technology solution. In terms of information security, it enables the State of Tennessee to be proactive in preventing security threats that propagate through messaging technologies. Centralization provides consistent policies and procedures for electronic messaging communications and the capability to enforce those policies and procedures statewide. Next, the solution provides the capability to securely send and receive information that is deemed confidential outside the State's network, such as protected health information.

### ***Section D: Realized return on investment, short-term/long-term payback (include summary calculations)***

The enterprise messaging solution for the State of Tennessee has provided very measurable cost savings across the board. There are two main categories of a positive return on investment for this environment. The first can be illustrated in terms of cost avoidance and hard dollars. Each

## State of Tennessee NASCIO Award Nomination 2006 Enterprise Architecture

spam message that makes its way past the organization's gateway costs the state money. The actual cost of each individual message is miniscule, but with an estimated 60% of all e-mail messages qualifying as spam or malicious content (approximately 120,000 per day), the constant flood of unwanted messages is of grave concern. The Ferris Group estimates that within unfiltered messaging environments the average employee spends 30 minutes each day dealing with spam, equating to 115 hours per employee, per year. Based on interviews with 82 Fortune 500 companies, Nucleus Research claims the average annual cost per employee of dealing with spam is now \$1,934. Specifically, within the State of Tennessee, if we take those estimates with our internal considerations and figures we end up with a cost of \$2,826 per employee. If we take the survey figures of approximately 115 hours wasted dealing with spam per year per employee the State of Tennessee's messaging solution provides \$99 million in total annual cost savings. If we take an even more conservative approach, and cut the estimated time dealing with spam (in an unfiltered messaging environment) in half, and assume only half of all State employees spend time dealing with spam we still see a very significant figure in the total annual cost savings calculations. In addition to employee productivity, capacity is also a major cost factor. If the State of Tennessee did not implement a messaging platform complete with a security and spam filtering solution the State would have had to double the number of post offices, currently at 71, at a cost of \$6,000 per post office server, or spend approximately \$426,000. That "fix" would be similar to buying larger buckets to bail water out of a sinking ship instead of fixing the hole causing the leak. This would only have bought the State more time given the fact that 60% of the messages we receive are categorized as spam. This means that every 2 to 3 years Tennessee would have had to dump another \$426,000 to increase post office capacity servicing the enterprise as well as add FTEs as the environment scaled. If we extend that out to 6 years worth of investment and scale, including the cost of the non-filtered environment, productivity loss (using the conservative estimate), and additional FTEs, it yields a long-term cost estimate surpassing \$26 million. The one time cost of the messaging solution, with anti-virus services, spam filtering services and secure e-mail delivery services manageable by 3 FTEs is less than \$1.5 million. For the purposes of this document, some maintenance costs have been omitted from these calculations, as they are relative to scale within each environment.

The second is a slightly less measurable return on investment analysis. It can be illustrated in terms of information security and potential financial impact of exposures due to risk, or soft dollar analysis. Information security and risk is a difficult ROI to illustrate because it deals with probability and some of the areas blend into hard dollar analysis. However, the technology industry has unfortunately had enough time to see real hard dollar impacts of security incidents propagated through insecure messaging services, i.e. Melissa or MyDoom. One of the primary vectors for malicious code propagation is the Simple Mail Transfer Protocol (SMTP) which all mail servers use to communicate. As the graph above illustrates, the State's messaging solution prevents thousands of malicious code injection attempts a day through this solution. In 1999, according to Computer Economics, the total financial impact of Melissa was estimated at 1.50 billion USD. The MyDoom worm gained the distinction of being the fastest spreading Malware attack ever, and according to Computer Economics, reached 12,000 systems per hour at its peak. The financial impact of MyDoom in 2004 was estimated at 5.25 billion USD.

The State of Tennessee has had its share of messaging based attacks. To its credit, the State's enterprise messaging solution has mitigated those types of threats down to a manageable exercise that generally only comes around with 0-day exploit based attacks. The State has filtered several hundred "Trojan horse" malicious code packages attached to an e-mail message which, if they were to get through and get to someone with access to financial systems, protected health information, or sensitive law enforcement information, the potential losses could be immeasurable in terms of dollars and may even result in the loss of life when considering the criticality of the systems and data used to service State citizens.