

---

**State of Maine**



**Current Information Technology (I.T.) Environment**

**January 2013**

---

## Table of Contents

Table of Contents .....	2
1. Introduction .....	3
2. Backup & Recovery.....	3
3. Storage .....	3
4. UNIX .....	3
5. Oracle Database .....	4
6. Oracle Middleware .....	4
7. IBM Mainframe .....	4
8. Client Technology Services.....	4
9. File Services .....	6
10. Windows Web Hosting.....	7
11. Remote Desktop Services (Terminal Services) /Citrix Application Delivery .....	8
12. MS SQL Server.....	8
13. Virtualized Windows x86/x64 .....	10
14. MS SharePoint .....	10
15. eGovernment.....	13
16. Applications .....	14
17. GIS Services.....	16
18. File Transfer.....	19
19. Network.....	19
20. Print.....	21
21. DNS.....	22
22. Directory Services.....	22
23. Security .....	22

## **1. Introduction**

This document describes the current I.T. environment of the State of Maine. No reference to this document is complete without citing its effective date. This document is strictly about the technology environment and not about the rates, which are posted elsewhere.

## **2. Backup & Recovery**

OIT standard backups are done with backup software purchased from CommVault. These backups are submitted at 7:00pm and run when resources are available throughout the night, finishing before 7:00am the next morning on weekdays. The Backup Group works with business users and technical support staff to work out special backup schedules when needed. Tape libraries with LTO-3 and LTO-4 drives are used to create tapes for offsite and long term storage. Magnetic libraries are used for some backups that require faster backup speeds or have small retention needs. CommVault's "continuous data replicator" product is used to replicate data from remote locations to Augusta where it is backed up. Less of this is being done as the data is being moved into Augusta.

Yearly CommCell failover testing is conducted between the CommCell at CMCC and the one at Sewall as well as off-site data storage checked to see that it aligns with the business needs for recovery point objectives (RPO) and recovery time objective (RTO) as identified in the business impact analysis (BIA).

We continue to explore options for off-site data rotation for D/R and retention purposes. Off-site data retention is analyzed to ensure it meets the agencies requirements and a tiered storage rate is allowing agencies the flexibility and scalability to meet their data retention needs.

With the consolidation of the datacenters we have full backup integration with our CommVault backup solution as the only offering.

## **3. Storage**

We offer a private cloud solution of tiered storage, data management and de-duplication at the NAS level, which includes user shares and applications shares. Data center replication is available for NAS based storage.

We have two datacenters consolidating all SOM storage onto the EMC series of arrays (NAS & SAN) allowing us to achieve full storage integration.

## **4. UNIX**

We offer physical and virtual servers in Solaris or Linux variants. Virtualization allows standardization of the operating system versions, adherence to the standard security model, and provide consistent OS level patching. All of this supports the goal of reducing the number of UNIX operating systems variants.

## **5. Oracle Database**

All Oracle databases run on commodity hardware, reducing the overall environmental consumption footprint. Databases run in an Oracle RAC configuration establishing a sustainable infrastructure with a focus on fault tolerance, security, scalability and integrated enterprise-wide monitoring. We have established a Center of Excellence to improve the overall quality of application delivery and simplify operational support. We encourage continual advancement of database versions to deliver technology that meets the business demands.

## **6. Oracle Middleware**

We run on commodity hardware, centralized and consolidated on all Oracle Application servers and Oracle Fusionware Suite products. We encourage continual advancement of Middleware versions to deliver technology that meets the business demands. Moving away from Oracle Application server is a key effort of the continual advancements initiative.

## **7. IBM Mainframe**

The IBM mainframe continues to support critical business applications for the State of Maine Department of Administrative and Financial Services. The CIMS application functions currently performed on the mainframe are expected to be migrated to another platform by 2Q/2013. A long-term effort to replace the HR Payroll system is in its early phases. The preparation, issuance and awarding of an RFP to procure a replacement payroll system is targeted to be completed in 2013. Upon selection of a vendor, it is estimated that the new enterprise HR system would be in place within three to five years. The new system would replace an outdated system as well as address requirements that are not currently supported by the existing system. During this period, plans to replace or retire the current TELCO application should be undertaken. Upon completion of the migration of these remaining applications off of the IBM mainframe, this application hosting environment will be decommissioned, concluding thirty to forty years of mainframe computing in Maine State government.

## **8. Client Technology Services**

We currently use Windows XP and Office 2010 and have stringent internet access with tight security. One of our biggest tools and assets is the implementation of SCCM. This has changed our way of doing business and allows us a vehicle to reach and repair our customers far exceeding our current SLAs and thus beginning to allow us to standardize our imaging process.

### **Client Devices**

Each device maintains a minimum of 3 gigs of memory, multi-processing processor, high definition video, and a minimum hard drive size of 160 gig. We have standardized on a single device offering for laptops and desktops, and no longer provide a high/standard offering. We perform our own warranty work on all devices. The PC Build Center has developed and implemented an inventory tracking program to assist in managing stock items. A power management program is in place to manage the behavior of monitors in

the fleet. This has resulted in energy cost savings, allowing the state to achieve a gold environmental award level status.

### **Client Software**

SCCM gives us the ability to upgrade to newer versions of software allowing us to maintain current releases on all devices. We have at a minimum on all devices: Windows XP, Internet Explorer 8, and Office 2010. Software installs are increasingly being performed remotely, greatly reducing the time to install software. Major upgrades to standard software offerings are now handled remotely, and through the RFC process. Client Technologies has begun to work with the Active Directory group to build the necessary infrastructure to allow the management of software deployment in a role-based distribution model. An inventory system is in place, as well as a software reconciliation program to ensure that all software in use by our customers is licensed.

### **Client Security**

Internet access is restricted to sites required for job function, and is now handled through Group Policy. Client Technologies has implemented the United States Government Baseline Computer (USGBC) standards on Internet security. These settings are managed through Group Policy. An exception process is in place to disallow users or groups from inclusion to these policies if needed. A major initiative was undertaken to standardize installs of the encryption software in use by the State of Maine (Pointsec). This has led to remote management of the encryption system, as well as better control of the security it provides.

### **Client Services**

We provide services to our customers that are unparalleled in customer service, effectiveness, and quality. Remote capabilities allow greater troubleshooting. Our goal is to provide 75% first call resolution. Our service level agreements are written to best suit the customer needs and it is our goal to maintain an 85% or better 'met' on all service level agreements.

### **Client EPO**

The administration of EPO for all desktops now entails a partnership with Client Technologies. In working with the security group, Standard Operational Procedures have been developed to streamline the processes of implementing new versions of the anti-virus systems, as well as developing its usage through patch management and add-on implementation.

### **Client GPO**

All desktop group policy is co-administered by Client Technologies and the Server Support group. This allows us the ability to manage the environment to the security level outlined in this document. An increasing number of user accesses of programs and external devices are being managed through group policy.

### **Client Call Center**

The Call Center is a virtual call center utilizing VPN tunnels. This allows us greater flexibility for coverage and provides us with a seamless business recovery plan. All ticket entries and call troubleshooting is standardized for streamlining and increased response time. With tools such as SCCM, Team Viewer, EPO Console, and other tools, the Call Center works toward a 75% first call resolution.

### **Client Field Technicians**

Client Technologies' improvements in managing imaged computers, the processes in requesting devices, and re-evaluation of stock levels have been an initiative for Customer Support. These changes to our process greatly reduce costs associated with deploying, migrating, and provisioning desktops and laptops throughout the state. It saves time and reduces human error over traditional PC deployments. It reduces end-user downtime by automating the deployment process and increases IT efficiency through automated, repeatable deployment tasks. Through these processes we have the ability to allow a greater ratio of technician to customers. This has allowed us to establish a greatly needed Research and Development team that focuses solely on customer requests for new software, new revisions, new upgrades, and package deployment.

## **9. File Services**

File service is provided using standard Microsoft drive mapping. Applications store essential data on servers or EMC storage device, no applications are allowed to run on the file server or EMC storage device and both types of device are accessed using fully qualified DNS names. Vendors should not assume that desktops are backed up. File servers are physically distributed in order to manage WAN segment loads and access latency.

Each user is allocated space for dedicated storage that is accessible only to that user and those others that have been approved by the user. A common area is allocated where files that are shared by all users in a workgroup can be placed and all members of the workgroup have full access to that area. Other data paths could be allocated based on request.

All centrally-administered storage spaces are maintained either on standard Windows Server 2003/2008 operating system, EMC storage device or other applicable environments (UNIX, NAS, SAN), based on best practices for the respective data type, including regularly scheduled backups. Through attrition we will replace old operating system servers with current operating system platform. The backup protocol is full backups once a week with incremental backups on the remaining days. Weekly tapes are retained for five weeks with the last weekly tape of each month retained for one year. If a longer retention is required, then it must be negotiated and paid for separately. No local desktop backup is offered, therefore, all data of value should reside on the centrally-administered storage space.

HP is the prime server hardware OEM, the preferred product being the Proliant DL or ML series depending on the project. The disk sub system is configured using raid technology. All servers are sized to handle peak loads demands. 2 fans, 2 power supplies, and 2 NICs are utilized for fault tolerance (teaming if required) and a 3<sup>rd</sup> NIC configured for backup (CommVault) purposes. ILO (Integrated Lights Out) is utilized for monitoring and remote reboots and HP Insight Manager for predicting hardware failures. All servers are monitored through Plixer WebNM, which is an agent-less, web-based monitoring and alerting tool for servers and network devices. WebNM provides a central overview of uptime and availability and performance data. Alerting options are highly configurable and can notify a pager, email, or cell phone. WebNM supports WMI, syslog, Event Log, and SNMPv1, v2, and v3. There exists a minimum 30-day lead time for implementing servers and other equipment into any data center. This process defines power, HVAC, rack, and other requirements.

## 10. Windows Web Hosting

**(disclaimer all applications would need to be migrated to the supported environment. Code will need to be updated to run on IIS 7.5 or above)**

Intranet: INET is a Windows 2008 server, running Internet Information Services (IIS) 7.5. INET provides hosting for agency intranet web sites. The server is located on the State's WAN and no external publishing to the internet is provided. Secure Socket Layer (SSL) is available. INET supports all current versions of the ASP.NET framework (2.0, 3.0, 3.5, 4.0 and above). Webpage publishing is done via FTP. In accordance with the Web Standards, both Macromedia Dreamweaver and Contribute are supported for content publishing. An INET test server (identical configuration to the INET production server) is also available for testing purposes.

Two IIS environments are provided for Internet/Intranet .NET applications: Gateway.maine.gov and Gateway.state.me.us.

Gateway.maine.gov supports all current versions of the ASP.NET framework (2.0, 3.0, 3.5, 4.0 and above). The environment consists of Windows 2008 R2 servers, running Internet Information Services (IIS) version 7.5. The servers reside in the State's DMZ. Secure Socket Layer (SSL) is available. Webpage publishing is done via FTP.

Gateway.state.me.us supports all current versions of the ASP.NET framework (2.0, 3.0, 3.5, 4.0 and above). The environment consists of Windows 2008 R2 servers, running Internet Information Services (IIS) version 7.5. Secure Socket Layer (SSL) is available. Webpage publishing is done via FTP.

## **11. Remote Desktop Services (Terminal Services) /Citrix Application Delivery**

Citrix and RDS allows for the distribution of native desktop applications from a controlled and centralized environment. Citrix/RDS gives poor performing Client-Server applications the ability to be offered across the State network. The enterprise environment consists of: Windows 2003/2008R2 operating systems running Citrix Presentation Server 4.5, Citrix XenApp 5.0, and RDS configured to interact with the State's Active Directory, load balancing, high availability, failover and redundant hardware is available. Citrix XenApp (formerly Citrix Presentation Server) is an application publishing product that allows users to connect to applications from central servers.

## **12. MS SQL Server**

The Enterprise SQL environments consists of the following:

### **SQL 2005 Database Services**

Production:

2 DL585 Servers  
4 2 Core AMD64 CPU  
32 GB RAM  
EMC SAN disk arrays for storage

Dev/Test:

1 DL585 Servers  
4 2 Core AMD64 CPU  
32 GB RAM  
EMC SAN disk arrays for storage

### **SQL 2008 R2 hosting environment.**

OLTP Services.

2 DL380 G7  
2 6 core CPUs  
96 GB RAM  
EMC SAN disk arrays for storage

SQL 2008 R2 HA DB Cluster.

2 DL380 G6  
2 4 core CPUs  
72 GB RAM  
EMC SAN disk arrays for storage

SQL 2008 R2 Reporting Services and Analysis Services

Production:

## SoM I.T. Environment

2 DL 380 G6 Servers.  
72 GB RAM.  
2 4 core cpus  
EMC SAN disk arrays for storage

SQL 2008 R2 Database, Reporting Services and Analysis Services

DEV/TEST:

SQL 2008 R2 DB (This server does double duty for OLTP and OLAP dev and test)

1 DL380 G6  
72 GB RAM  
2 4 core CPUs  
EMC SAN disk arrays for storage

SQL2008 R2 DB Batch Services (SSIS)

1 DL360 G5  
2 2 core CPUs  
16 GB RAM  
Local disk arrays for storage

### **CJIS SQL 2008 Hosting Service**

1 DL380 G5  
2 2 Core CPUs  
16 GB RAM  
Local storage arrays for DB storage

### **OIT recommendations and best practices for hosting SQL Server.**

A minimum of a production and test are required for each application. Our SQL 2008 cluster accommodates HA requirements. This requires no additional configuration on the client. (Unlike Mirroring) Storage is provided by the EMC disk arrays. Disks are configured such that RAID 1+0 is utilized for database log files and data files. The environments are configured to optimize performance.

Active Directory integrated security is the preferred option. Services such as Reporting Services, Web, and OLAP services will be added as satellite services that may rely on the Enterprise OLTP.

SQL database accounts are the less preferred method of accessing SQL Server databases. Applications should be designed with this in mind. Also applications should be designed using the principal of least privilege. System Administrator (SA) access will not be granted. Remote access to the operating system is prohibited.

The CJIS SQL Server has been deployed for applications that have high security requirements. All applications utilizing this server need to meet the CJIS security requirements. This server runs SQL 2008 Standard edition X64 in an effort to keep costs

down. This environment also has Analysis Services and Reporting Services available. The environment is to serve the high security needs of certain Public Safety applications.

SQL Analysis Services and SQL Reporting Services will accommodate a variety of reporting and general BI needs. This environment can scale out to accommodate heavier loads as they arise. This environment will support High Availability through the use of the Alteon load balancers and a backend report repository and temp db on the new SQL 2008 cluster. This design also allows the reports to be deployed only once and each "leg" of the HA BI solution will be updated at the same time as each instance of Reporting Services is using the same reporting database.

Batch services allows the customer to manage the job(s) themselves. If customer chooses not to manage the job(s) OIT will charge a monthly rate to administer job(s) based on per job.

Applications should be designed to allow support from application support personnel with limited permissions. (Without SA permissions)

Applications Support will need to provide a contact for each database deployed as well as a business contact. OIT hosting services include backups and restores and server level items. All other administration tasks are expected to be performed by a competent Application Support specialist..

### **13. Virtualized Windows x86/x64**

The preferred platform for Windows x86/x64 systems is VMWare Vsphere 4.\* or current version. The operating system guest is Windows 2008 R2 Server or current OIT supported Windows Server Version. Virtualization has been adopted to dramatically reduce power and cooling costs, reduce the need for expensive data center expansion, increase operational efficiency, and capitalize on the higher availability and increased flexibility that comes with running virtual workloads. The goal is for I.T. to be well-positioned to rapidly respond to ever-changing business needs.

### **14. MS SharePoint**

SharePoint 2010 is available for agencies on the internal State of Maine network. The environment consists of multiple front-end web servers and a backend server that handles service applications.

All SharePoint features are available. Below is a list of some of the SharePoint features that are available.

Costs: Agencies that require enterprise features must purchase Enterprise Client Access Licenses (CALs) for their users in addition to the chargeback-rate per user. Agencies are responsible for Site Collection administration. Storage costs are billed at the published storage rate.

**Collaboration Features:**

**Tasks** – Create, assign and track the progress of tasks.

**Announcements** – Share news and information with users or team members.

**Calendars** – Create and share calendars with team members, create meetings and manage recurring events.

**Document Libraries** - Share and manage related documents through a library of multiple documents.

**Form Libraries** - Create and Share XML or InfoPath based Forms.

**Contacts** - Share contact information with your team so they can keep in touch.

**Surveys** - Create a Poll that your team can vote on, with customizable survey options.

**Discussion Forums** - Discuss related issues with your team and easily references resources.

**Links** - Share useful links and external information with your team.

**Custom Lists** - Create a custom list with the information and data you need to share.

**Alerts** - Receive alerts as they happen or on a schedule notifying you when changes happen.

**Microsoft Office Integration** - Integration with the Office Suite including offline support for Access, Outlook and content support for Excel, PowerPoint and Word.

**Outlook Integration** - Document libraries can be taken offline into Outlook 2007/2010 folders and changes synchronized back to SharePoint when you are online.

**RSS Feeds** - RSS Feeds are automatically generated for any list, allowing for easier notification of changes.

**Document Versioning** - Major and Minor version numbers are supported when documents are updated.

**PDF Support** - Adobe PDF documents are indexed and the contents are searchable within your SharePoint site.

**Manage Document Metadata** - Store different types of content with similar metadata in the same library.

**Content Management Features:**

**Web Parts** - Lists, Libraries and Functionality can be added to a Web Part and shared within anywhere within your site.

**Picture Libraries** - Share Images or Photos with your Team.

**Blog Pages** - SharePoint allows you to set up a fully functional blog site within your site.

**Wiki Pages** - Set up, maintain and share information amongst team members using a Wiki based knowledge management.

**Search** - The new portal search engine technology which allows you to search lists, libraries, content and even within documents.

**Mobile Access** - You can view and update tasks lists, blogs and other information direction from mobile devices. Simply add /m onto the end of any URL to view a mobile-friendly presentation of the page.

**Gantt Chart View** - Tasks, Issue and Project Issue lists can be view graphically giving you a quick view of a project's status.

**Predefined Workspaces** - Many different pre-defined workspaces are available and can be provisioned as a sub-site, including Meeting Workspaces, Issue Tracking, Blogs, Wikis, Project Tracking, Document Review and many more!

**Tree View and Breadcrumbs** - Users can more easily identify where they are on the site.

**Site Management:**

**Sub-Sites** - Create sub-sites or sub-webs as you need for different teams, projects or goals.

**File Blocking** - Restrict specific file types from document libraries if needed.

**Site-Based User Management** - Control access to a site or sub-site by restricting which users will have access.

**Granular User Permissions** - Permissions can be defined as deep as an individual document, list or library, granting you as much control as you need.

**Help on every page** - Built in Help menus help users who are getting started learn what they need to know.

**Recycle Bin** - The site administrator can now restore any deleted items, ensuring nothing is lost.

**SSL Encryption** - A shared SSL certificate allows for improved security when you need it.

### **Customization Features:**

**Browser Based Customization** - Customization - By simply using a Web Browser like Internet Explorer you can get started customizing your site right away.

**Themes** - Built-in themes allow you to customize the color and design of your site quickly and easily.

**Master Pages** - Using master pages you can create a single page template and use it as the basis for multiple pages. Master pages allow you to apply your own personalize style and layout to your SharePoint site, and work with all Application Templates, allowing you to create more advanced customizations.

**Application Templates** - With over 40 application templates you can easily find a solution that suits your needs. Application templates can be deployed automatically through sub-site creation.

**SharePoint Designer Support** - Advanced Customization and Design can be accomplished using Microsoft Office SharePoint Designer.

**Workflow** - Custom workflows can be built for different content types or libraries and can be triggered when items are added, modified, or initiated manually.

## **15. eGovernment**

### **Statewide Unified External Directory & Authentication**

Located at [www.public.maine.gov](http://www.public.maine.gov), with underlying Microsoft Active Directory, this is designed to serve as the definitive external authentication for use services across the state. At present, those interacting with the state must do so via multiple authentication silos. The definitive external authentication seeks to simplify and improve user experience, while increasing the security and integrity of online service delivery.

### **External URL Harmonization**

**Maine.gov is the official Internet brand for Maine State government.** It is in the best interests of the state citizenry to present the state government service portfolio as one unified whole. To implement this, the State will acquire a proxy server capable of harmonizing external URLs so that customers are unaware of the heterogeneity of the internal naming & hosting environment.

### **Web Applications Architecture**

Web applications should fully conform to the state's applications architectural design with clear separation between the User Interface, Business Logic and Data. The user interface and presentation logic may reside on the portal but the remaining two layers: Business Logic and Data, must reside on secured backend systems. At present, the location of backend systems is slightly prejudiced in favor of the OIT-hosted environment. However, due to the continued growth of secure, commoditized cloud services, it is expected that many backend systems will progressively relocate to the cloud.

## 16. Applications

The State emphasizes modularity, componentization, and reuse capability in applications, and modules within applications. Applications must strive toward: 1) making use of an existing functionality, or 2) create reusable functionality/components when none exists.

All State Applications should be clearly decomposed into at least three tiers:

- User Interface (U.I.) or Presentation Tier: Typically the presentation tier is the gateway between the end user and the Business Tier. It consists of the artifacts related to the input-output devices, such as the video screen, the keyboard, the mouse, the speakers, etc. The U.I. either resides in the customer-access device, or is downloaded into it on-demand. The U.I. tier may also contain any rules-engines that derive the U.I. so long as its sole purpose is to facilitate and enrich the user experience. It should never encroach upon the Business Tier.
- Business Tier: Typically the broker between the Presentation Tier and the Data Tier. Business Tiers contain the transformation rules that implement the Use Cases. A Use Case is a well-defined sequence of actions undertaken jointly by the user and the application that produces a predictable result of value to the user. The transformation rules should be amenable to being isolated from a particular application via componentization, input-output parameterization, and minimizing the use of static (global) variables.
- Data Tier: Depending on whether the purpose is transactional or analytical, may consist of Configuration Data or Transactional Data or Transactional Safeguards or Specialized Decision Data Structures. It is understood that Transactional Safeguards are created for the sake of data integrity, fine-grained security, audit, etc., and where a proprietary database-specific procedural language may be used. But it is also a matter of prudence and judgment to keep the Transactional Safeguards compact enough to not encroach upon the Business Tier. The default expectation remains that with the exception of the Transactional Safeguards, ALL data access will be accomplished via ANSI-compliant SQL. It is further understood that the design and structuring of the Data Tier will be different depending upon whether the purpose is transactional or analytical.

## SoM I.T. Environment

- Additionally there may be interface or integration tiers which may be incorporated into or maintained separate from the Business Tier.

The art and science of building good applications is too rich to be recapitulated here. That said, the State places a premium on the following:

- A clear separation among the tiers with well-defined interfaces between them.
- All Business Logic should be anchored from well-defined user roles.
- In terms of long-term enterprise asset management, the two tiers that matter the most to the State are the Business Logic and the Data.
- As long as U.I. and U.I. Logic remain thin, and do not encroach upon the Business Logic, the State remains agnostic of their implementation technologies. However, the purely browser-based U.I. still remains the first preference, as opposed to any U.I. that relies upon a native operating system.
- Any enhancement, or extension, to an existing application is best accomplished in the native technology of the original application, provided, of course, the native technology is one of the approved ones in the Bricks. If the native technology happens to be in either Containment or Retirement, then stakeholders should initiate a disinvestment plan.
- Critical to breaking down program silos and improving the capability of agencies to work together is to structure the Business Logic in terms of Web Services. Web Services are small, self-contained chunks of logic that expose Business tier Objects and methods through interfaces over HTTP(S), and can be mixed and matched a la carte without any limit. In this configuration, applications no longer have monolithic business logic dedicated to them. Rather, applications become a collection of loosely-coupled, self-contained Web Services, fronted by a thin U.I. layer. It is a strategic goal of OIT that all State applications migrate toward Web Services.
- Microsoft Active Directory is the fiduciary directory for all internal I.T. resources within the State. The State has just launched an external Active Directory implementation (Public.Maine.Gov), and to the extent feasible, all *new* external applications are expected to leverage it for external authentication. All State applications should be fully Active Directory-aware. Specifically, they should be capable of consuming all authentication services from the Active Directory. It should be noted that this does not automatically imply single sign-on. For reasons of security, confidentiality, etc, applications are free to require as many authentications as necessary. However, for each such authentication, the user will furnish their Active Directory credentials, as opposed to any application-specific credentials. Re: authorization, applications are expected to maintain their own repositories of roles. However, wherever two or more applications require sharing authorizations, they

should consider federating such authorizations to a neutral repository, with the system-of-record granted complete control to manage such authorizations.

- Applications should scrupulously guard against standard security vulnerabilities, such as Injection Attacks, Buffer Overflows, Cross-site Scripting, etc. At a minimum, they should perform thorough vetting and filtration of all user-input before passing them into the Business Tier, and the same for back-end outputs, such as errors, warnings, exceptions, etc., before presenting them back out to the U.I. In the same vein, applications should strictly avoid invoking dynamic queries from interactive forms in favor of explicit methods and procedures. User requests should never invoke any operating system calls, or command interpreters, or SQL interpreters, etc. Beyond such minutiae, security considerations should be baked into each tier right from the design, rather than bolted on post-facto.
- It is theoretically possible to enforce individual-level audit at either the Business Tier or the Data Tier, or even both. The most foolproof solution is to enforce it at the Data Tier as part of a Transactional Safeguard, but that requires propagating all application user identities into the Data Tier. When application user identities are propagated into the Data Tier, it is critical to ensure that the Data Tier identities do not allow any access to the underlying data outside of the application context. While this makes the audit foolproof, the one deficiency of this approach is that there cannot be any pooling of the connection between the Business Logic and the Data. Whereas, embedding the individual-level audit exclusively within the Business Tier, and then using a shared/generic application-identity to access the Data Tier, can facilitate connection pooling into the Data Tier, thereby making the data access more efficient. But, in that case, the entire burden of the audit rests within the Business Logic; Not that it cannot be done, but it is a high burden, and there is no safety net.
- It remains an explicit goal of the State to foster the embedding and cross-fertilization between spatial and non-spatial applications. Please refer to the G.I.S. section for more details.

In closing, the State will continue to expect higher degrees of modularity, componentization, and reuse in its applications. More specifically, there will be a greater emphasis on Web Services, Service Oriented Architecture, and Software as Service.

## **17. GIS Services**

The enterprise GIS infrastructure consists of several components: Web Mapping, Application Programming, Database, and Desktop. Each of them is elaborated further below.

### **Web mapping**

There are currently two mapping environments: ArcGIS Server and MapServer.

ArcGIS Server is the current ESRI offering for web mapping and web GIS services. This is a strong tool for deploying web services, especially useful for geoprocessing and geocoding services.

MapServer is an open-source web mapping platform for lighter weight web mapping applications, which also doubles as a WMS server. Maine makes wide use of MapServer for hosting imagery. We develop simple web mapping viewers using the GeoMoose template.

Google Earth Enterprise is a visualization tool used for customized interfaces with data in the Google Earth format. This is widely used in our emergency mapping field.

Free mapping applications such as Google Maps, Yahoo Maps, MapQuest, Google Earth, etc. are also allowed, but the State cannot guarantee the reliability and sustained availability of these tools. Use of such free tools is an implied agreement with their terms of use. The State cannot accept any liability or obligation with respect to these services, and users are strongly encouraged to deliberate the underlying terms and conditions before adopting them. Due to the possible transient nature of such services, they are not recommended for uses in applications intended to promote the preservation of life, safety, and property. Also, the underlying data behind Google Maps is less accurate than the 911 Roads Layer maintained by the State. State programs consuming Google Maps are strongly urged to consider using the 911 Roads Layer where appropriate.

### **Application Programming**

There are numerous development options available to build GIS based applications. Current approved languages include C# .NET, VB.NET, ASP.NET, Java, PHP, Python, HTML and JavaScript. Approved and supported programming languages are maintained independent of GIS toolkits.

Specific GIS or map based tools that have been approved for use to build application include tools from Esri (specifically ArcGIS Server Web API for JavaScript, ArcGIS Online Web API for JavaScript, ArcObjects 10.x without VBA), tools from Google (specifically Google Maps JavaScript API, and Google Earth Enterprise), open source tools (specifically MapServer/PHP/GeoMoose), and the Oracle Spatial PL/SQL API. We are containing the use of certain GIS toolkits and discourage the proliferation of applications dependent on them. These include ESRI's ArcGIS Server Application Development Framework (ADF), ArcGIS Server Web API's for Flex and Silverlight and ArcObjects integrated with VBA.

OGC-compliant standards are supported. To the maximum extent possible, applications should rely upon currently supported tools and use open standards (such as the OGC standards). Proprietary or third-party tools can only be used after a thorough testing and vetting cycle, and the lack of alternatives to a critical business need.

### **Database**

## SoM I.T. Environment

Spatial data are stored using ArcSDE (now known as ArcGIS Server Basic Edition enterprise license), primarily on Microsoft SQL Server database. There are three core locations for ArcSDE: the Maine Office of GIS (MEGIS), the Department of Transportation (DOT), and the Department of Environmental Protection (DEP). DEP operates Oracle on Solaris, DOT and MEGIS on Windows. The State largely uses direct-connect database connections rather than actually running SDE servers. There are many client-side databases which are hosted in Microsoft Access, ESRI file-based geodatabases, DBF files, or INFO databases. The enterprise is working on standardizing all its data into ArcSDE 10.1, with the exception of certain DOT applications which still require ArcSDE 9.2.

### **Desktop**

There are three main desktop GIS suites: ArcGIS, MapInfo, and Google Earth.

ESRI ArcGIS is the most widely-used desktop GIS suite, and is deployed either through desktop installs or Citrix (200-300 users). Most users are now on version 10.1. DOT still has some requirements for ArcGIS 9.2 to interface with their ArcSDE 9.2. Several custom tools are written for ArcGIS in Python.

MapInfo is used primarily by Conservation, Agriculture, Maine Housing Authority, and Baxter Park Authority. This suite is available either through either desktop installs or Citrix. Most users are on version 9 or 10. This software is in containment.

DeLorme XMap is used primarily by law enforcement personnel, such as forest rangers, game wardens, marine patrol. This software is deployed via desktop installs. This software is in containment.

Google Earth is used primarily by DEP, MEMA, PUC, and to some extent by other agencies. Usage of this suite is protected to grow and integrates with our Google Earth Enterprise platform.

ArcView 3.x is obsolete technology which still has some applications, but is being phased out, and will become de-supported in the future.

The MEGIS site ([www.maine.gov/megis](http://www.maine.gov/megis)) provides internet access to internet applications and services, packaged GIS data for download, and additional State GIS information.

The Maine GeoLibrary Portal ([geolibportal.usm.maine.edu](http://geolibportal.usm.maine.edu)) is hosted by the University of Southern Maine, and provides metadata search services, and the ability for organizations to upload metadata and shapefiles. It runs on GeoNetwork open-source software. This platform is not directly supported by the State, but is in use at the university system.

## **18. File Transfer**

The State of Maine uses MoveIT DMZ Enterprise from Ipswitch.

Move-it allows for FTPS (ftp over explicit SSL) and SFTP (ftp over SSH) connections. In addition to the secure transmission of data, the data is stored securely on the server using its own folder and file structure making it independent of the operating systems' file system. Move-it DMZ has the capability for secure messaging and allows the ability to use active directory to authenticate clients. Data transmission is done either by using the ftp protocol or by the web using HTTPS. The first method requires the client to have ftp software. The latter method allows the client to connect using any web browser.

## **19. Network**

The State's networks have evolved into a robust, converged solution for voice, radio, video, and data elements. Security, manageability and reliability requirements result in the implementation of access control, traffic, shaping and advanced network architectures while next generation applications, social media and multimedia experiences drive the need for more bandwidth and multicasting technologies. New technologies, protocols and processes contribute to an ever-improving network experience for end users and a concurrent improvement in productivity.

This report touches briefly on the major elements of our network and how they support functional requirements, technology changes, application/service growth, service model changes and consolidation requirements.

### **Wide Area Network**

We utilize a third party carrier provided MPLS Carrier Ethernet Service (CES) for network connectivity to edge sites outside metropolitan campus areas state-wide. Offerings run from 5Mbps to 1GBPS, depending on need and ability to pay for enhanced bandwidth; bandwidth-on-demand is available in the CES cloud, so automated short-term bandwidth increases are possible. This provides a cost-neutral upgrade in base bandwidth and future scalability at remote sites, and eliminates the concept of remote core sites. All traffic from WAN sites is delivered via ring-based fiber at 1 or 10 Gigabit per second (Gbps) to two core sites, configured for high availability failover using Virtual Router Redundancy protocol (VRRP). Quality of Service (QoS) is currently deployed, and the underlying model is adapted to be in line with emerging needs.

### **Microwave**

With the completion of the MSCCommNet radio project, the backbone microwave system provides transport for IP based LMR radio traffic and system management services. Designed to interconnect with the evolving legacy WAN, the microwave system provides alternate voice, video and data routing to critical public safety sites around the state. Conversely the WAN provides alternate transport for IP based radio

traffic (RoIP) as well as Simple Network Management Protocol (SNMP) based system management services.

### **Local Area Networks/Metropolitan Area Network**

The State uses common manageable switch and wireless fabrics with extended protocol support including LLDP, 802.1x, etc.. It will be enhanced by new technologies as needed, including wireless in all current and new variants. Wireless coverage based on 802.11a/b/g/n continues to expand to meet the growing needs of mobile workers, business partners, citizen customers and wireless ready devices.

### **Data centers**

Switching and load-balancing/application delivery controller (LB/ADC) architectures are 10Gbps centric hardware with 1Gbps support; implementations are 1Gbps centric with 10Gbps support. All connectivity in the Sewall Street data centers are HA so that loss or planned outage of any single piece of hardware or media will not result in a service failure. Virtualization in application switching (LB/ADC) environments supports and enhances the virtualization of servers. New protocols under development by IEEE (802.1Qbg, 802.1Qbh, etc.) are embedded in the switch fabrics. Application-layer QoS has been adopted in line with policy.

### **High Performance and Availability Core**

The State owns and operates a Dense Wave Division Multiplexing (DWDM) core including at a minimum the two data centers, the Cross Office Building (COB), and the Riverview Psychiatric Center complex (RPC, formerly AMHI). Implemented as a ring topology, this allows large numbers of fully protected circuits inter-connecting fiber-attached locations at the four campuses at speeds from 10Mbps to 100Gbps using any protocol (Ethernet, fiber channel, etc.), with 50ms or less failover in the event of fiber failure. The core routing infrastructure is fully redundant so that failure or planned maintenance of single major components will not cause a service outage.

### **Network Services**

- IPv6 and multicast support (these are not co-dependent features) are technically possible within the State's entire network; functionality may or may not be deployed actively to clients and servers depending on policy and/or requirements.
- Link-based encryption has been replaced by client/server implementations; firewalling at edge sites is available now at most WAN sites. Policy-based routing is available now and in the future as required.
- Directory services have been transformed to an AD integrated centralized LDAP authentication platform. All AD domains have been collapsed into organizational units under a single HA root domain. WINS has been phased out, and DNS

security extensions (DNSSEC) implemented. The current Infoblox grid has been fully upgraded.

- The extranet provides fully load balanced connectivity to multiple Internet connections.
- A single remote access methodology based on the Juniper remote access cluster is scaled as needed to support addition concurrent user loads as a result of the decommissioning of IPRS based dial in service, limited use of CheckPoint's SecuRemote and increases in telecommuting and home workers.
- Voice, radio, video and data traffic converge onto a single delivery network. Session Initiated Protocol (SIP) trunking integrates legacy digital/analog networks into the converged Voice over IP (VoIP) solutions.

### **Network Management**

- The State has implemented proactive network performance data collection systems that lead to lower customer downtimes and improved performance. IPFix/Netflow/SFlow reporting is ubiquitously available at most network levels. Analytical toolsets exist to provide better end-to-end insight into and optimization for many application issues.
- Quality of service management is provided to allow for the efficient transfer of data throughout the network.
- Network management functions are isolated from possible access by unauthorized entities. Networks configuration, change and compliance management continue to be implemented for all network elements.

## **20. Print**

Within the realm of our current Print Platform responsibility, OIT EOM has two sites to support; the CMCC site and the State Street site (Central Print).

CMCC has 1 IKON Canon printer and Central print has two IKON Canon printers, 3 Xerox printers. We have Xerox and IKON contracts.

Central Print came about as a result of a 'secondary' reorganization between OIT and BGS, whereby an exchange was made of the BGS Central Print location for the OIT CMCC Mail Center. The idea was to have the Mail Center under the control of the State Postal Service and to have Central Print within the realm of EOM's HSP environment.

- All State printing services exist within the Central Print environment with 5 High Speed Printers.
- A single Print Platform is available to the User community creating a consistency that helps Central Print improve on efficiencies.
- We reach out to all State Agencies, working with existing customers and to establish new customers providing a wide variety of printing solutions.

## 21. DNS

- DNS is critical to the overall performance of the network and the Internet. Today's DNS structure allows for many vulnerabilities such as DNS spoofing, hijacking, DoS attacks, cache poisoning, etc. Moving to secure DNS (DNSSEC) is the IETF's effort to eliminate these vulnerabilities.
- The Enterprise Directory Services group is 80% complete with the migration to DNSSEC. All re-architecting and role-changing within our environment has been accomplished. We need only turn DNSSEC on, and perform the required upstream key exchanges.

## 22. Directory Services

- Internal Directory Services (AD) is a Single Forest with multiple Child Domains populated with resources (e.g., printers) and security principals (user or computer accounts and groups).
- External Directory Services (AD) – Has been created. It is the Enterprise Directory Services Group's intent to utilize the "pristine" external public AD forest for Publicly accessible application

## 23. Security

Security is inextricably baked into the design and architecture of all I.T. assets. In terms of process and governance, cross-boundary security coordination, advance vulnerability detection and remediation, internal and external audits have been progressively strengthened. The Enterprise Security Team has completed the following programs and initiatives:

- Performed Security Assessments on infrastructure assets
- Performed Security Penetration Assessments on web applications
- Performed Security Vulnerability Assessments of desktop systems to assure compliance with federal regulatory agencies.
- Implemented Department of Homeland Security Network IDS
- Coordinated the removal of malware infections throughout the Executive Branch

## SoM I.T. Environment

- Centrally managed Enterprise Anti-Virus solution for Executive Branch and some Non-Executive Branch Agencies
- Increased Web Browsing Security through Site Advisor deployment
- Manage physical access permissions for OIT staff and OIT areas
- Routinely audited physical access permissions
- Implemented Security Awareness Training for DAFS
- Wrote and maintained security policies and rules and provide advice and consultation to other branches of OIT regarding best security practices.