State of Colorado

Information Technology Enterprise Architecture Standards

Version 1.3

July 16, 2004

Commission on Information Management (IMC)
Governor's Office of Innovation and Technology (OIT)

Revision History

Version 0.1	Draft Created	Architecture Advisory Committee	05-20-03
Version 1.0	Revised	State CIO's Review	06-16-03
Version 1.0r1	Approved	Commission on Information Mgmt	06-20-03
Version 1.1	Revised	State CIO's Review	09-04-03
Version 1.3	Revised	State CIO's Review	07-16-04

Executive Summary

The State of Colorado's Office of Innovation and Technology convened an advisory panel of industry experts in enterprise architecture to recommend a World-class enterprise architecture that would enable the State to provide services to the State's constituents and to manage it's applications and data independent of organizational structure.

The advisory panel recommends a Web Services architecture for the State of Colorado. This architecture provides the independence of data and application management desired by the State. Further, the standards which support a Web Services architecture are mature and well supported by vendors and products. This ensures the State can leverage free market competition as it pursues construction of systems which conform with enterprise architecture and supporting standards.

Architecture Advisory Board Members

Bannon Bednarcyk	IBM
Vasanthan Dasan	Sun Microsystems
Alan Grose	Microsoft
Jeet Jagasia	Microsoft
Rick Lebsack	IBM
Gordon McGowan	Sun Microsystems
Marshall Presser	Oracle
Jeff Sherrard	State of Colorado
Steve Williams	Cisco Systems

Table of Contents

1.0 Purpose

This document presents the Web Services architecture recommended by the Enterprise Architecture Industry Advisory Panel. This document also identifies the technical standards required to enable the architecture.

2.0 Goals and Objectives

The State of Colorado's Office of Innovation and Technology convened an industry advisory panel of enterprise architecture experts to recommend a world-class enterprise architecture to support the future direction of the State of Colorado. This direction is to provide one-stop customer service, in person, over the phone, or via the web, 24 x 7.

To support these enterprise objectives the enterprise architecture must provide:

seamless data sharing across the enterprise,
seamless application sharing across the enterprise,
seamless, heterogeneous datacenter management,
24 x 7 service delivery,
standards based vendor competition, and,
stability over a 10-year period.

The advisory panel was asked to leverage the work done in industry, in other states, and by the Federal Enterprise Architecture effort.

3.0 Scope

The Enterprise Architecture Industry Advisory Panel was asked to identify the critical technical standards that must be present across all State departments, to support the State's future goals and objectives. This effort focused specifically on the technical architecture and did not address the business or information layers of the enterprise.

The business layer of enterprise architecture typically addresses the organizations structure and the way in which it interacts with its customers. The information layer addresses the use of information within the enterprise, where information is created, stored, modified and destroyed.

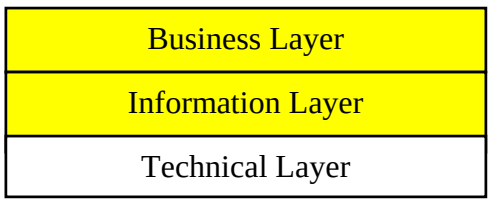

Figure 3.1 Enterprise Architecture Scope

4.0 Relationship to Other Standards

This document and the standards contained within this document, compliment the existing information technology standards that have been previously approved by the Commission on Information Management.

If conflicts arise between this standard and a past standard, this document shall take precedence. If conflicts arise between this standard and federal standards, the federal standards shall take precedence.

Nothing in this document shall excuse any State agency from meeting its security requirements established in the Health Information Portability and Accountability Act (HIPPA).

This document coordinates with the following State standards:

ADA Standards	1/12/01

5.0 Policy and Governance

These standards establish common criteria for the assessment of programs, projects, and initiatives within the departments, agencies, and divisions of the State of Colorado. It is not assumed or intended that all departments will be able to implement these standards at the same rate.

It is the intent of these standards that every State agency:

1) Self assess compliance with these standards at least annually,
2) Assess all new programs, projects and initiatives, against these standards,
3) Use these standards in procurements, to the greatest extent possible.

The Office of Innovation and Technology shall maintain the statewide scorecard showing the assessment results for each department. This scorecard will assist the Commission in its review and approval of information technology investments and progress towards compliance over time.

Exceptions to these State standards require the prior written approval of the Commission on Information Management.

6.0 Technical Architecture

The goals and objectives of the State are common in industry and government enterprises. A web services architecture is widely used by these enterprises. Web services are broadly supported by the standards community and the vendor community. This architecture is directly applicable to the goals and objectives for the State of Colorado.

6.1 Web Architecture

The State of Colorado will become a highly interconnected governmental enterprise. The constituents of the State will interact in person, over the phone and via the web. Services will be provided to the constituents independent of the internal organization of the departments, divisions and agencies. The State's Web Architecture, shown in Figure 6.1 below, fully supports this future vision.

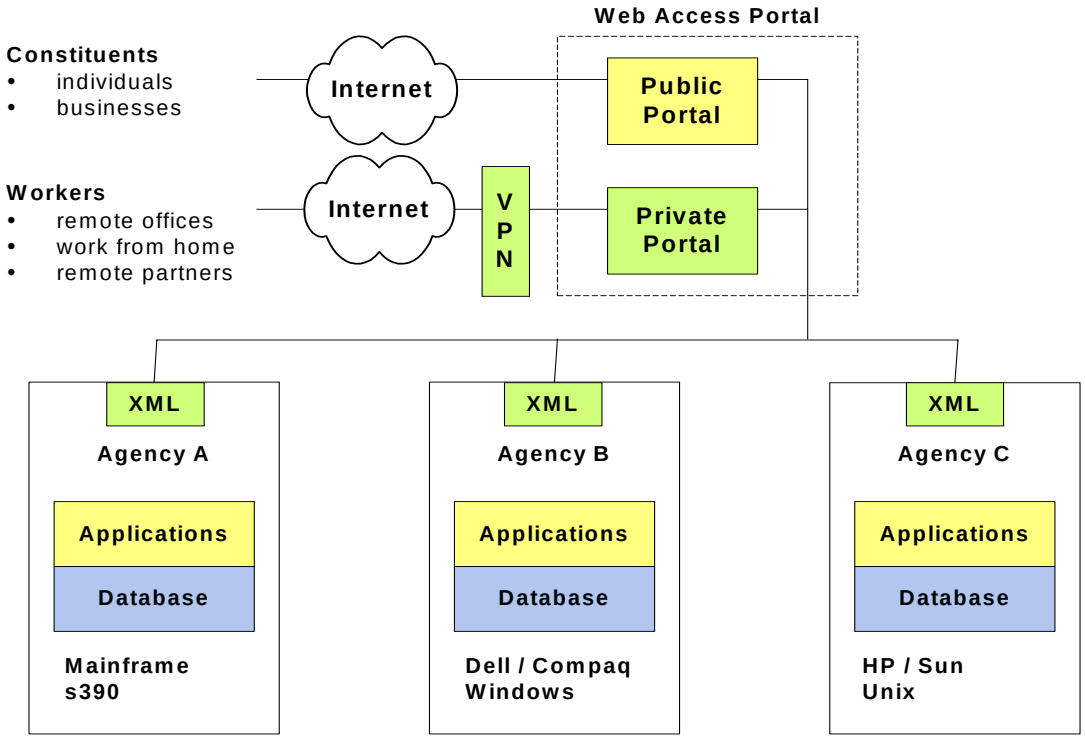

Figure 6.1 State of Colorado – Web Architecture

The technology and standards necessary to realize this vision exist, are supported by products available from multiple vendors, and are in common use within industry.

6.2 Network Architecture

A highly reliable, high bandwidth network is essential for the success of any technology-enabled enterprise. Users, whether they are constituents, employees, vendors or partners expect to be able to access services anytime. The network must be designed to provide not only the access, but also the security, reliability and response-time required by its users.

7.0 Supporting Standards

A stable body of industry standards support enterprise web services architectures. The critical standards necessary to enable this architecture are presented in this section.

7.1 Network

A secure, well-organized network that provides reliable connectivity and performance, is required for a web services architecture. See section 7.8 – Security, for additional security requirements.

7.1.1 IP Network

All State computers (desktop, server, mainframe) must be accessible via an IP network.

7.1.2 IP Address Allocation

IP address blocks must be centrally managed for the Enterprise. IP addresses must be allocated geographically following standard sub-netting rules. Each geographical region should aggregate to a single route.

7.1.3 Local Network

Local, unroutable, internal IP addresses that conform with RFC 1918, shall be used on end user devices, to the greatest extent possible.

7.1.4 Routing

State Networks must use a standards based Interior Gateway Routing protocol (IGP) to connect to the MNT. Acceptable protocols are OSPF, EIGRP and RIPv2.

Multi-Protocol Label Switching (MPLS) must be used in the State WAN to provide logical separation of network traffic.

7.1.5 Domain Name Services (DNS)

DNS names registration must be centrally managed and administered. Domain name servers must be redundant and geographically distributed. Machines will be accessed via DNS names to the greatest extent possible.

7.1.6 Reverse Proxy

All State webservers must utilize reverse proxy servers or virtual IP load balancing technologies. See Figure 7.8.5 - Three Firewall DMZ for a graphical representation of the placement of a reverse proxy server.

7.1.7 Dynamic Host Control Protocol (DHCP)

DHCP must be used for all desktop, laptop, and remote systems. Fixed IP addresses shall only be used for network devices and servers.

7.1.8 VPN (Virtual Private Networking)

Remote access to internal State computational resources must only be provided through secure VPN connections. These connections shall require three (3) element authentication, as a minimum (e.g. an identifier – username, something you know – password, something you have – SecurID code). These connections must provide encrypted exchange of information through the entire life of the connection.

7.1.8.1 Remote Access VPN

Access VPNs encompass analog, dial, ISDN, digital subscriber line (DSL), mobile IP, and cable. Access to internal State computational resources may only be provided through secure VPN connections.

7.1.8.2 Site-to-Site VPN

Network nodes requiring secure connectivity between themselves and their organizational hub, or where secure connectivity over the Internet is more cost effective and efficient than private WAN connectivity.

7.1.8.3 Extranet VPN

Links between customers, suppliers, partners, or communities of interest to the State Intranet over a shared infrastructure may be provided through secure VPN connections.

7.1.9 Firewall

All State computers must be protected from public access through the use of stateful Firewalls. These firewalls must follow the philosophy to deny all access except those protocols, ports, and addresses that are explicitly permitted. Firewall policies shall be clearly documented, reviewed, and updated annually.

7.1.10 Wireless Access Points

No wireless access points or bridges shall be allowed to connect to the State's network without providing:

802.1X authentication & authorization for access,
WEP based encryption, and,
a non-broadcast SSID.

No wireless Access points are allowed to connect to Data Center network segments.

7.1.11 Network Administrator Security

Default accounts that provide administrator or "super user" privileges on network equipment shall be protected.

7.1.11.1 Default Administrator Passwords

Default administrator passwords shall be changed on installation.

7.1.11.2 Administrator Passwords Strongly Formed

Administrator or super-user passwords shall be strongly formed.

- The password must contain at least one number, one lower case character and one uppercase character.
- The password cannot contain any dictionary word greater than or equal to four (4) characters.
- The password cannot be changed to any of the three (3) previous passwords.
- The password must be at least eight (8) characters long.

7.1.11.3 Administrator Passwords Changed Every 90 Days

All administrative passwords shall be changed at least every ninety (90) days, and on departure of any person with knowledge of those passwords.

7.1.11.4 Administrator Password Storage

Administrative passwords shall not be stored anywhere on the file system in text readable format; this includes operational batch scripts, application programs and password files.

7.1.11.5 Log Failed Admin Access Attempts

All failed attempts to gain access to user accounts with administrative privileges shall be logged and reviewed at least weekly.

7.2 Datacenter

The State has a duty to secure the Public's data and provide for its availability to continually perform the State's business. All data of record stored by the State, must be contained in a clearly identified datacenter. Each datacenter must provide:

a) Datacenter Operational Services
b) Environmentals (Power, HVAC, Fire)
c) Network (bandwidth, utilization, latency, redundancy)
d) Security (physical, network)
e) Backup / Restore Capabilities and Services
f) Business Continuance

7.2.1 Datacenter Operational Services

Every State datacenter must provide a description of the datacenter operational services provided. On-site vs. off-site support must be clearly identified

7.2.2 Datacenter Environmentals

Every State datacenter must provide controlled environmentals to include: a) conditioned and/or uninterruptible power, b) heating and cooling, and c) fire suppression.

7.2.3 Datacenter Network Access

Every State datacenter must provide network access for mission critical Enterprise data. Network access shall be characterized by bandwidth, utilization, latency and redundancy.

7.2.4 Datacenter Physical Security

Every State datacenter must provide physical security that limits access. This must constitute the second layer of physical access between the public and State owned resources.

7.2.5 Datacenter Network Security

Every State datacenter must provide network security as specified in Section 7.8 - Security.

7.2.6 Datacenter Backup

All State computers (desktop, server, mainframe) must have system, application, and data backup plans and procedures documented. The plans and procedures shall be reviewed and updated annually. These plans must include: 1) periodic backups, 2) periodic movement of backups to offsite storage, 3) periodic recovery testing.

7.2.7 Datacenter Disaster Recovery or Business Continuance

A disaster recovery plan or a business continuance plan must be created

for each Department or Agency's computational resources (desktop, server, mainframes, network). The plan must include a business case showing the impact to the State and it's constituents. The plan shall be reviewed and updated annually.

7.3 Web Access

A major goal for the State is to provide one-stop customer service. Internet standards provide a sound technical foundation for that goal. These originate in standards bodies and exist to ensure interoperability between different technologies and are supported by multiple vendors.

Another goal of the State is 24 x 7 service availability. Technologies inherent in web infrastructure are commonplace in the web services market today. Web applications can be easily spread across multiple application servers. If one server fails, another server takes over for it. An edge server can dispatch the browser requests across as many servers as necessary. This provides for 24 x 7 availability.

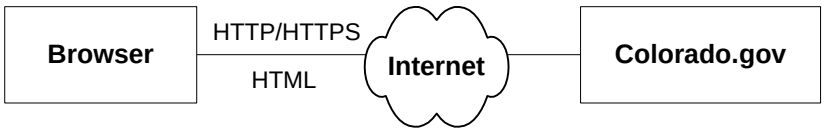

Figure 7.3 Web Access

7.3.1 HyperText Markup Language (HTML)

HTML (HyperText Mark-up Language) interface is the standard for user interfaces. All new development efforts are required to design an HTML interface as the systems primary user interface.

7.3.2 EXtensible Markup Language (XML)

XML (Extensible Markup Language) is the standard format for server-to-server data interchange. All new development efforts are required to design XML interfaces, define data interchange documents via Document Type Definitions (DTD), and implement services to accept requests and provide replies to valid DTD's.

7.4 Email

State Email systems must support the following standards:

Simple Mail Transport Protocol (SMTP),
Post Office Protocol (POP) and/or Internet Mail Access Protocol (IMAP), and,
Multipurpose Internet Mail Extensions (MIME)

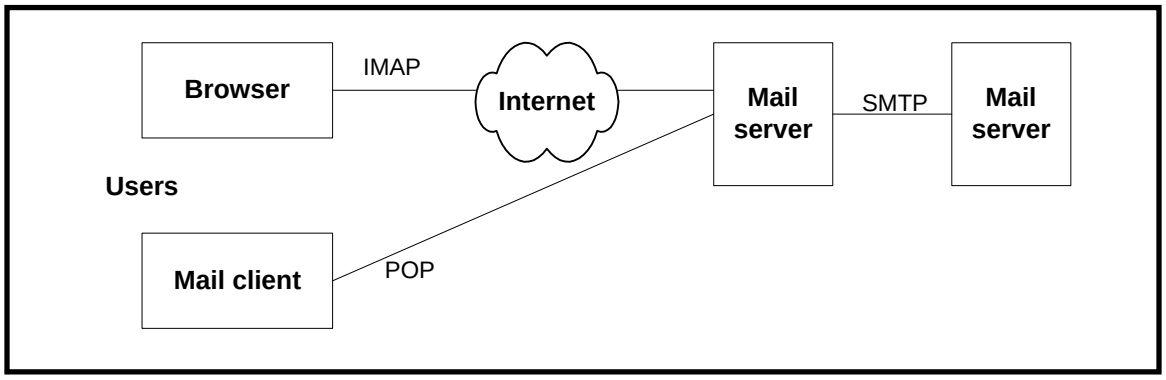

Figure 7.4 Email Architecture

7.4.1 Simple Mail Transport Protocol (SMTP)

SMTP is the standard for exchange of email between servers. All State email servers must support SMTP.

7.4.2 Post Office Protocol (POP) and/or Internet Mail Access Protocol (IMAP)

All State email servers must support POP3 or IMAP4 for client access.

7.4.3 Multipurpose Internet Mail Extensions (MIME)

All State email servers must support MIME content.

7.5 Identity Management

Large number of users, constituents, employees, partners and suppliers are allowed to access systems and information in the State's web enabled enterprise. Identity management is the capability to manage these varied identities and levels of access, across the enterprise's varied environments.

An identity management system must include administrative and self-service interfaces that simplify and automate managing the addition (provisioning) and removal (deprovisioning) of users and their ability to access systems.

Delegated administration allows multiple administrators to assist in the provisioning and management of users, allowing the main administration group to delegate some authority to departments or agencies, as necessary. This allows the large problem of user identity to be divided into manageable pieces.

7.5.1 Directory

A solid directory foundation is required infrastructure necessary to enable mission-critical security and authentication.

7.5.1.1 Lightweight Directory Access Protocol (LDAP)

All State directories must support the LDAP standard.

7.5.1.2 X.500 Directory Services Model

All State directory structures must follow the x.500 standard.

7.6 Database

At the heart of the enterprise architecture is data storage, manipulation, and retrieval. In order to provide a high quality and consistent level of data service within and between agencies, the State will mandate that all new database management system satisfy the following conditions. Database systems that do not meet such standard will at minimum provide gateways that enable their data to be shared by relational systems using SQL as the standard means of interaction.

7.6.1 Open Database Connection / Java Database Connectivity (ODBC/JDBC)

ODBC/JDBC is the standard for database connectivity. All State database systems must provide for ODBC and/or JDBC connections.

7.6.2 Structured Query Language (SQL)

Structured Query Language (SQL) is the standard for database queries. All State database systems must support SQL.

7.6.3 Relational Database Management System (RDBMS)

All State databases must be relational database management systems.

7.6.4 RDBMS Administrator Security

Default accounts that provide administrator or "super user" privileges in an RDBMS shall be protected.

7.6.4.1 Default Administrator Passwords

Default administrator user passwords shall be changed on installation.

7.6.4.2 Administrator Passwords Strongly Formed

Administrator or super-user passwords shall be strongly formed.

- The password must contain at least one number, one lower case character and one uppercase character.
- The password cannot contain any dictionary word greater than or equal to four (4) characters.
- The password cannot be changed to any of the three (3) previous passwords.
- The password must be at least eight (8) characters long.

7.6.4.3 Administrator Passwords Changed Every 90 Days

All administrative passwords shall be changed at least every ninety (90) days, and on departure of any person with knowledge of those passwords.

7.6.4.4 Administrator Password Storage

Administrative passwords shall not be stored anywhere on the file system in text readable format; this includes operational batch scripts, application programs and password files.

7.6.4.5 Log Failed Admin Access Attempts

All failed attempts to gain access to user accounts with administrative privileges shall be logged and reviewed at least weekly.

7.7 Application

Common application development methodologies ensure consistency of application development and support. Tool-based development enables tool-based operations and support, which improves systems long-term maintainability, reducing total cost of ownership.

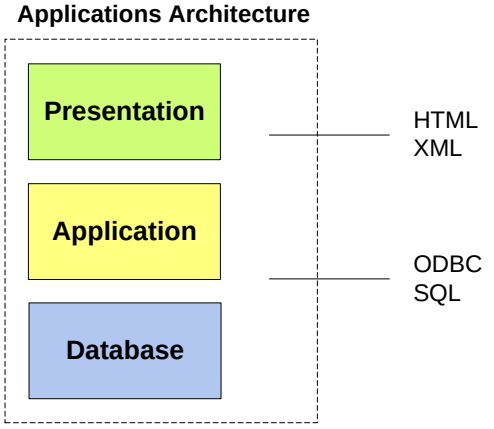

Figure 7.7 Application Architecture

7.7.1 n-Tier Application Development

All State web applications shall be developed following the n-tier development model to clearly separate presentation (look and feel), from the application (business logic), from the database.

In addition to the advantages of distributing programming and data throughout a network, n-tier applications have the advantage that any one tier can run on an appropriate processor or operating system platform and independently of the other tiers.

7.7.2 Tool Supported Software Development

All State applications development shall be supported by software engineering tools for the management of requirements, design, and software development.

7.7.3 Analysis and Design

All analysis and design must be performed using object oriented analysis (OOA) and object oriented design (OOD) tools and techniques.

7.7.4 Uniform Modeling Language (UML)

In order to facilitate precise communication, an open source independent modeling language is required. UML is widely supported for this purpose. Every State application must have an accompanying Use Case models, Class Diagrams, Component models and Deployment Diagram.

7.7.5 Configuration Management

Management of software assets (models, code, documentation, test cases, etc) shall be centralized in a configuration management repository.

7.8 Security

The State has an obligation to its citizens, businesses, employees, and its agencies and departments to provide security of information residing in and traveling to or from state operated computers.

7.8.1 Encryption

All State computational resources using encryption shall use approved encryption algorithms and key lengths. (112 or 168 bit 3DES , 128 bit SSL, or AES – Advanced Encryption Standard) for data in transit as well as data in place. The use of proprietary encryption algorithms is not allowed for any purpose.

7.8.2 Intrusion Detection Service (IDS) – Network Based

All publicly accessible, State computers must have a network based intrusion detection service capable of combating unauthorized intrusions, malicious Internet worms, bandwidth attacks and e-Business application attacks.

The IDS must provide stateful pattern recognition, protocol analysis, traffic anomaly detection, and protocol anomaly detection.

The IDS must monitor all IP protocols (e.g. TCP, UDP etc).

The IDS must statefully decode application-layer protocols (e.g. FTP, SMTP, HTTP, DNS, RPC, Telnet etc).

The IDS must interact with firewalls and other network devices to actively shunt attacks and provide event notification.

7.8.3 Virus Detection

- All State computers shall have software capable of detecting known viruses and worms and informing system administration personnel which files are infected. This software must allow for periodic update of its virus list from an external source.

7.8.4 Wireless Security

Access to State of Colorado networks via unsecured wireless communication mechanisms is prohibited. Only wireless systems that meet the following criteria are approved for connectivity to State networks.

This standard covers all wireless data communication devices connected to any State internal network. This includes any form of wireless communication device capable of transmitting data. State wireless connections must:

- Maintain point-to-point hardware encryption of at least 128 bits.
- Support strong user authentication which checks against an external database such as TACACS+, or RADIUS.
- 802.11b (Wi-Fi) devices must be LEAP/EAP/PEAP compliant.

7.8.5 DMZ

A DMZ protects internal networks from the public network. A DMZ shall be part of all State systems that allow for access to or from the Public Internet. The DMZ must be hosted in a datacenter (see Section 5.2).

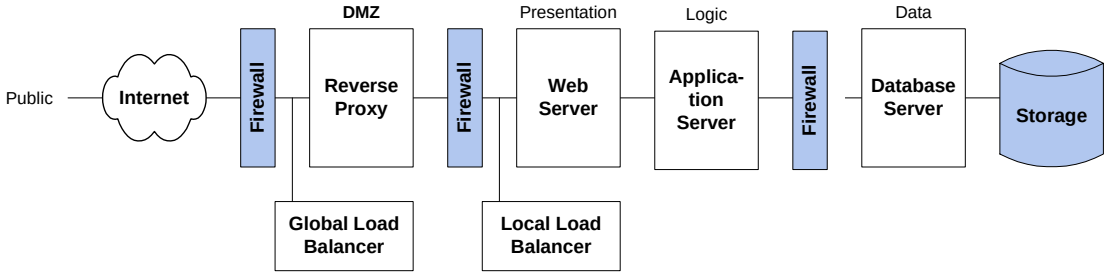

Figure 7.8.5 Three Firewall DMZ

7.8.6 Authentication/Authorization/Accounting

TACACS+, Radius, or Kerberos authentication must be used for access to all State network resources and devices. Access to systems will require 3-element authentication (e.g. an identifier – username, something you know – password, something you have – SecurID code). Roles and privileges must be maintained in an LDAP compliant data store. Access to State computing & networking facilities and devices will be audited by a combination of hardware and software components that determine which persons are using the system.

7.8.7 System Administrator Security

Default accounts that provide administrator, root, or "super user" privileges on computer equipment shall be protected.

7.8.7.1 Default Administrator Passwords

Default administrator passwords shall be changed on installation.

7.8.7.2 Administrator Passwords Strongly Formed

Administrator passwords shall be strongly formed.

- The password must contain at least one number, one lower case character and one uppercase character.
- The password cannot contain any dictionary word greater than or equal to four (4) characters.
- The password cannot be changed to any of the three (3) previous passwords.
- The password must be at least eight (8) characters long.

7.8.7.3 Administrator Passwords Changed Every 90 Days

All administrative passwords shall be changed at least every ninety (90) days, and on departure of any person with knowledge of those passwords.

7.8.7.4 Administrator Password Storage

Administrative passwords shall not be stored anywhere on the file system in text readable format; this includes operational batch scripts, application programs and password files.

7.8.7.5 Log Failed Admin Access Attempts

All failed attempts to gain access to user accounts with administrative privileges shall be logged and reviewed at least weekly.

7.8.8 Web Security

The State shall us HTTPS (SSL) and WS-Security to ensure secure transmission of information to and from the public Internet. SSL provides transport level security. WS-Security provides message level security for web services. WS-Security describes enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication.