TITLE 1 GENERAL GOVERNMENT ADMINISTRATION
CHAPTER 12 INFORMATION TECHNOLOGY
PART 11 ENTERPRISE ARCHITECTURE

1.12.11.1 ISSUING AGENCY. Information Technology Commission, 404 Montezuma, Santa Fe, NM 87501.
[1.12.11.1 NMAC - N, 06-15-2005]

1.12.11.2 SCOPE. This rule applies to the enterprise architecture of the state of New Mexico (SoNM) and all IT projects or programs undertaken by agencies. This rule applies to any state government body or public entity that would like to become a member or utilize services within the enterprise data center.
[1.12.11.2 NMAC - N, 06-15-2005]

1.12.11.3 STATUTORY AUTHORITY. NMSA 1978 Section 15-1C-5 and 15-1C-8.
[1.12.11.3 NMAC - N, 06-15-2005]

1.12.11.4 DURATION. Permanent.
[1.12.11.4 NMAC - N, 06-15-2005]

1.12.11.5 EFFECTIVE DATE. The effective date is 06-15-2005, unless a later date is specified at the end of a section.
[1.12.11.5 NMAC - N, 06-15-2005]

1.12.11.6 OBJECTIVE. The purpose of this document is to establish rules, standards, and policies for the enterprise architecture for the SoNM.
[1.12.11.6 NMAC - N, 06-15-2005]

1.12.11.7 DEFINITIONS. As used in this policy.

A. Address block means a contiguous group of internet protocol (IP) addresses.

B. Addressing resolution means a method for resolving differences between computer addressing schemes. Address resolution usually specifies a method for mapping network layer (layer 3) addresses to data link layer (layer 2) addresses.

C. Address resolution protocol means a protocol for mapping an IP address to a physical machine address that is recognized in the local network.

D. Application administration account means any account that is for administration of an application.

E. Agency network means networks that are managed by individual agencies and autonomous to state's core network.

F. Architecture means a logically consistent set of principles, policies, and standards that guide the engineering of state government's information technology systems and infrastructure in a way that ensures alignment with state government's business needs.

G. American registry for internet numbers (ARIN) means one of four regional internet registries. ARIN, founded in 1997, is a non-profit organization that registers and administers *IP numbers* for North America. ARIN is one of four regional internet registries.

H. Class A network means a binary address starting with 0; therefore, the decimal number can be anywhere from 1 to 126. The first 8 bits (the first octed) identify the network, and the remaining 24 bits indicate the host within the network.

I. Class B network means binary addresses that start with 10; therefore, the decimal can be anywhere from 128 to 191; (the number 127 is reserved for loop-back and is used for internal testing on the local machine**).** The first 16 bits (the first two octets) identify the network, and the remaining 16 bits indicate the host within the network. An example of a class B IP address is 168.212.226.204, where "168.212" identifies the network and "226.204" identifies the host on that network.

J. Class C network means binary addresses that start with 11; therefore, the decimal number can be anywhere from 192 to 223. The first 24 bits (the first three octets) identify the network, and the remaining 8 bits identify the host within the network. An example of a class C IP address is 200.168.212.226, where "200.168.212" identifies the network and "226" identifies the host on that network.

K. **Common service** means a function that may be in use or deployed in multiple agencies, whether they are using the same programs or people to perform the function or not.

L. **Consolidated service** means a function that is performed by a common group of programs or people for multiple agencies, under centralized control and with agreed-upon standards, interfaces, and service level agreements.

M. **Consolidated service** means a function that is performed by a common group of programs or people for multiple agencies, under centralized control and with agreed-upon standards, interfaces, and service-level agreements.

N. **Cost recovery service** means a service that is charged back to the consumers of the service at a fully loaded rate to allow the provider to recoup all associated costs with providing the service.

O. **Current technology** means components that have met requirements of the EA - those components that should be used in deployment of technology solutions.

P. **Emerging technology** means products that have potential to become current components.

Q. **Enterprise** means that for this document, 'enterprise' refers to the executive branch of the government of the SoNM, including all business processes and IT support systems.

R. **Enterprise architecture** defines an enterprise-wide, integrated set of components that incorporates strategic business thinking, information assets, and the technical infrastructure of an enterprise to promote information sharing across agency and organizational boundaries; the enterprise architecture is supported by architecture governance and the allied architectures of business, information, technology, and solution architectures.

S. **Enterprise project** means a project with the purpose of delivering new or modifying existing services to many stakeholders within the state.

T. **General funded service** means a SoNM service funded through general fund tax dollars.

U. **Internet protocol (IP) address** means a 32-bit address used to indicate a specific network and host on the internet or within a local network. The address is usually seen in decimal representation in the form *nnn.nnn.nnn.nnn*, where *nnn* can be any number between 0 and 255.

V. **Internet protocol security (IPSec)** means a set of protocols developed by the internet engineering task force (IETF) to support secure exchange of packets at the IP layer by encrypting a 1.18.361 NMAC authenticating all IP packets. IPsec has been deployed widely to implement virtual private networks.

W. **Internet protocol version 6 (IPv6)** means a standard intended to replace the previous standard, IPv4, which only supports up to about 4 billion addresses (4 x 109), whereas IPv6 supports approximately 3.4 x 1038 addresses, equivalent to 430,000,000,000,000,000,000 unique addresses per square inch of earth. The root domain has been changed to support both IPv6 and IPv4. It is expected that IPv4 will be supported until about 2025 to allow for bugs to be worked in support of new IP and wireless devices.

X. **Other-funded service** means a SoNM service that receives funding from non-SoNM sources or state funds other than the general fund, such as the road fund, federal government, or a locality.

Y. **Network address translation** means an internet standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the internet makes all necessary IP address translations by keeping IP addresses of network packets passing through a router or firewall. Hosts, which are behind a NAT-enabled gateway, do not have end-to-end connectivity. NAT serves three main purposes:

(1) provides a type of firewall by hiding internal IP addresses;

(2) enables a company to use more internal IP addresses (since they are used internally only, there is no possibility of conflict with IP addresses used by other companies and organizations); and

(3) allows a company to combine multiple ISDN connections into a single internet connection.

Z. **Passphrases** means that a public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

AA. **Private address** means a space that has been allocated via request for comments (RFC) 1918. These addresses are available for any use by anyone, and therefore the same private IP addresses can be reused. However, they are not routable - they are used extensively in private networks due to the shortage of publicly remittable IP addresses.

BB. **Request for comment (RFC)** means a series is used as the primary means for communicating information about the internet; some RFCs are designated as internet protocol.

CC. **SANS** means a sysadmin, audit, network, security, or SANS institute.

DD. **Self-funded service** means a SoNM service that, through its use, generates a stream of revenue sufficient to cover its on-going costs and to accrue monies to pay for future development and enhancement.

EE. **Service** (types of) - see 'common service', 'consolidated service', 'cost recovery service', 'general funded service', 'other-funded service', and 'self-funded service'.

FF. **Sunset technology** means components in use which do not conform to the ITEA and with a stated specific date set for discontinuance - indicating the date that the component will no longer be acceptable for use.

GG. **Twilight technology** means components in use, but which do not conform to the stated business/technical drivers; no date of discontinuance is identified - but not to be used for new development or new procurements; extensive modifications should be avoided.

[1.12.11.7 NMAC - N, 06-15-2005]

1.12.11.8 ABBREVIATIONS AND ACRONYMS:

A. **ARIN** means American registry for internet numbers
B. **ARP** means address resolution protocol
C. **CIO** means chief information officer
D. **EA** means enterprise architecture
E. **IETF** means internet engineering task force
F. **IP** means means internet protocol
G. **IPSec** means IP security
H. **Ipv4** means version 4 of the internet protocol
I. **ISDN** means integrated services digital network
J. **IT** means information technology
K. **ITC** means information technology commission
L. **ITEA** means information technology enterprise architecture
M. **LAN** means local area network
N. **NAT** means network address translation
O. **NM** means New Mexico
P. **NT** means new technology (predecessor of windows 2000 server)
Q. **OCIO** means office of chief information officer
R. **RFC** means request for comments
S. **SANS** means system administration, audit, network, security, or SANS institute
T. **SoNM** means state of New Mexico
U. **TCP** means transmission control protocol
V. **VPN** means virtual private networks
W. **WAN** means wide area network

[1.12.11.8 NMAC - N, 06-15-2005]

1.12.11.9 - 1.12.11.14: [RESERVED]

1.12.11.15 NETWORK. IP addressing.

A. The enterprise service provider will assign, document, and manage all address blocks of private, public, and reserved address spaces.

B. Agencies will manage and control all addresses within their block. Agencies will be required to submit current and accurate IP sub-net assignments and change control documentation to the enterprise service provider database on a real-time basis.

C. An agency core router will be configured to route only 10.0 and 164.64.0.0 addressing.

D. Private class A (RFC 1918) IPv4 is to be the named standard for all agencies and core networks to extend networks within the state that do not want to be routed to external sources with subnets of class B and class C.

E. Public Address.

(1) In the event that access is required to route to an external source, addresses must be public.

(2) The only public address range that will be advertised by the SoNM to the internet is the 164.64.0.0 class B address space assigned by ARIN.

F. The reserved address 1.18.361 NMAC.

(1) This reserved addressing will be limited to securing segregated voice transmission until an equally secure design is available with RCF 1918.

(2) Reserved addressing will not be implemented in the same autonomous RCF 1918 or public addressing.
[1.12.11.15 NMAC - N, 06-15-2005]

1.12.11.16 SECURITY. Password policy.

A. This policy establishes a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

B. Passwords must be at least eight (8) alphanumeric characters long.

C. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed at least every 6 months. Password changes will be addressed immediately by the password authority when personnel changes are made to staff that have root access.

D. Passwords must not be stored on unencrypted or other insecure forms (i.e., word document, post-its, labels, etc.).

E. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed periodically. The minimum change interval is every 4 months.

F. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

G. Passwords must not be inserted into email messages or other forms of electronic communication.

H. All user-level and system-level passwords must conform to the guidelines described below.

I. A password authority shall be established by the agency CIO or IT lead to disseminate passwords, facilitate as the gatekeeper for system-level passwords, and be the point of contact for password-related security breaches. Password may only be obtained or requested from the password authority of the agency.
[1.12.11.16 NMAC - N, 06-15-2005]

History of 1.12.11 NMAC: [RESERVED]