

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))), including, the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

A.R.S. § 41-712, establishes the Telecommunications Program Office (TPO) within the Arizona Department of Administration (ADOA) to provide a cost effective and efficient network infrastructure and program to serve the State of Arizona. This program is known as the Arizona Network (AZNET) that provides wide-area network services to better serve state agencies, departments, boards, commissions and the public. AZNET coordinates state and agency wide-area network designs and related secure implementations that support converged services, while accommodating traditional data, voice, and video services. AZNET also encourages further deployment of open systems based on targeted network architectures that use common, proven, pervasive, and industry-wide standards.

3. SCOPE

A budget unit is defined as a department, commission, board, institution or other agency of the state receiving, expending, or disbursing state funds or incurring obligations of the state including the Arizona Board of Regents but excluding the universities under the jurisdiction of the Arizona Board of Regents, the community college districts and the legislative and judicial branches (A.R.S. § 41-3501(2)).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each budget unit.

4. STANDARD

Budget Units that maintain an existing network infrastructure are considered grandfathered from migrating to the AZNET program. However, any significant changes to a Budget Unit's wide-area network infrastructure and related technologies shall give TPO/AZNET of ADOA a competing chance to implement the AZNET program, or portions thereof.

Additionally, budget units may also deploy network infrastructure that may be outside the scope of AZNET, but which should compliment the AZNET program and adhere to this standard. Such budget unit network infrastructure includes local area

elements and certain wireless networks as identified by the AZNET program.

The following sections in this standard incorporates open, industry standards to provide for common, scalable, interoperable, and secure network infrastructures that support converged services, as well as accommodating traditional data, voice, and video services. These flexible standards provide the infrastructure foundation for more effective sharing of common IT resources in addition to improving quality, usefulness, and efficiency of cross-agency applications and information throughout the State.

4.1. **Structured Cabling Systems:** Cabling installations for new buildings, major cable plant additions or modifications, building renovations or remodeling, shall meet all minimum requirements and mandatory criteria addressed in Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) Commercial Building Telecommunications Standards 568, 569, 606, 607, and applicable electrical codes.

- TIA/EIA 568-B.1, 2, and 3 standards specify a telecommunications cabling system for commercial buildings that will support a multi-product, multi-vendor environment.
 - The TIA standards for Commercial Building Telecommunications Cabling address cabling infrastructure design, installation, and field testing for copper and fiber network horizontal cabling, backbone cabling, and work areas.
 - Target categories provide additional requirements for copper network cabling in Paragraph 4.2 and fiber network cabling in Paragraph 4.3.
- TIA/EIA standards, while providing for the acceptance of newer cabling categories through addendums, do not remove earlier cabling categories from the standards. Cabling categories before 5e do not provide the necessary capability for converged services.
- The TIA/EIA 569-A standard for telecommunications pathways and spaces addresses floor loading, ceiling and perimeter pathways, conduit, and other aspects of routing cable throughout and between buildings for copper and fiber network horizontal cabling, backbone cabling, and work areas.
- TIA/EIA 606 standard provides a uniform administration scheme to manage telecommunication infrastructure.
- TIA/EIA 607 standard provides grounding and bonding requirements for telecommunications circuits and equipment.

4.2. **Copper Network Cabling:** Structured Cabling System installations for new and/or renovated buildings without cabling shall be Category 6 Unshielded Twisted Pair (UTP) as specified by TIA/EIA 568-B.2.1 Commercial Building Telecommunications Cabling Standards.

- Category 6 cabling is certified to carry up to 10 Gbps of data up to 100 meters. The cabling industry, TIA, and International Organization for Standardization/International Electrotechnical Commission (ISO/IEC)

support Category 6 cabling or better as the optimal choice to develop the Institute of Electrical and Electronics Engineers (IEEE) 10 Gbps Ethernet standard based on the rapid growth of Category 6 cabling installations in the marketplace.

- Category 5e cabling is acceptable when incremental additions to existing Category 5e cabling for major cable plant modifications and/or additions due to building renovations or remodeling are necessary.
- Category 6 link and channel requirements are backward compatible to Category 5e.
- Category 6 cabling, and existing Category 5e cabling, installed per TIA 568-B.2.1 standards, to the desktop allow most IP platform devices requiring power to operate without supplemental AC power in accordance with IEEE 802.3af Power over Ethernet (PoE) requirements.
- Category 5e patch cables used to connect platform client devices to Category 6 Structured Cabling Systems where throughput performance is constrained by the platform client device interface are acceptable.
- UTP shall be used unless specific issues exist, such as high EMI or long transport distances.

4.3. **Fiber Network Cabling:** Structured Cabling System installations for new buildings, major cable plant additions or modifications, building renovations or remodeling shall be either multi-mode or single-mode, depending on business unit requirements, as specified by TIA/EIA 568-B.3 and ISO/IEC 11801:2002 Commercial Building Telecommunications Cabling Standards.

- TIA/EIA-568-B series standards specify 50/125 micron multi-mode fiber for horizontal subsystems. 50/125 micron multi-mode or single-mode (8/125 micron) fiber is specified for vertical subsystems.
 - Multi-mode fiber transmits up to 10 Gbps Ethernet a distance of approximately 35 meters to 300 meters (50/125 micron), depending on the specific fiber and the Ethernet port characteristics. Single-mode (8/125 micron) transmits up to 10 Gbps Ethernet a distance of 2, 10, and 40 kilometers, depending upon specifications.
 - Single-mode fiber network cabling subsystems between buildings allow up to 10-Gbps Ethernet transmission rates over greater distances, as specified by the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) Series G.652 and ISO/IEC 60793 standards.

4.4. **Wireless Network Connectivity:** Shall be secure in accordance with *Statewide Standard P800-S830, Network Security*; use encryption technologies; be protected using Virtual Private Network (VPN) and firewalls, as necessary; and be compliant with IEEE 802.11x (Wireless Local Area Network (WLAN)), IEEE 802.15 (Wireless Personal Area Network (WPAN)), and IEEE 802.16 (Wireless Metropolitan Area Network (WMAN)).

- *Statewide Standard P800-S830, Network Security*, describes minimum requirements for providing secure and seamless interconnection of communication networks and systems.

- *Statewide Standard P800-S850, Encryption Technologies*, describes minimum requirements for ensuring the authenticity, integrity, confidentiality, and reliability of digital information.
- Security is being addressed in the transmission layer with the IEEE 802.11i standard and at the IP applications layer with standards- and policy-based authentication and access control. The Wired Equivalent Privacy (WEP) algorithm, which is part of the 802.11x standard, is susceptible to compromise; therefore, improved security methods should be considered. The WiFi Protected Access (WPA) standard and Protected Extensible Authentication Protocol (PEAP) with the IEEE 802.1x Network Port Authentication standard provides interim, improved security until approval and widespread adoption of 802.11i. In addition, vendor-specific, proprietary, security solutions may provide more enhanced interim security prior to approval and widespread adoption of 802.11i.
- Mobile IP provides an efficient and scalable mechanism to allow users to seamlessly roam among wireless networks. Using Mobile IP in applications such as VoIP, media streaming, and virtual private networking can be supported without service interruption when users move across network boundaries.
- Wireless Profiled TCP (WP-TCP) provides connection oriented services for developing applications that operate over wireless communication networks via the Wireless Application Protocol (WAP). Wireless Profiled TCP is optimized for wireless environments due to the emergence of high-speed wireless networks (e.g., 2.5G and 3G) and provides for large data transfers, end-to-end security (using TLS) and convergence with IETF protocols.
- Wireless client platforms utilizing VPN technologies to access internal networks and mission-critical software applications² improve security and decrease certain vulnerabilities inherent in unprotected wireless connectivity.
- Firewall technologies must be implemented at connection points between wireless and wire-based LANs additionally to reduce unauthorized access to internal networks.
- The IEEE 802 standards enable convergence of technologies and the development of an open-standards-based infrastructure for the Wireless Internet.
- The IEEE 802.11x standards form a family of specifications that define how WLAN equipment should be produced so equipment from different manufacturers can work together.
- The IEEE 802.11b and .11g standards operate in the unlicensed radio 2.4 GHz frequency band and provide up to 11 Mbps and 54 Mbps transmission speeds, respectively, for wireless connectivity.

² Mission-critical software applications are those that address health, life, and safety issues; provide critical public services; or have been prescribed by legal mandates.

- The IEEE 802.11g is backwards compatible with .11b allowing .11g and .11b devices to coexist in the same network (.11g devices' performance declines based on distance and number of wireless devices).
- The IEEE 802.11f Inter Access Point Protocol ensures interoperability between access points from multiple manufacturers.
- The IEEE 802.15.3 standard is designed for short-range (up to 50 m), very-low-power operation from 11 to 55 Mbps. The standard will provide quality of service, connection management, and advanced power management modes. The IEEE 802.15.2 standard addresses coexistence between WLANs and WPANs operating in the 2.4 GHz frequency band.
- The IEEE 802.16x standards address the “first mile/last mile” connection broadband wireless access for Metropolitan Area Networks, providing up to 155 Mbps transmission speeds. These standards provide for interoperability and coexistence of fixed broadband wireless access systems from multiple manufacturers in both licensed and unlicensed frequency bands. The IEEE 802.16x standards provide for quality of service to support the needs of different applications. IEEE 802.16 WMAN can coexist with IEEE 802.11x WLAN to provide a viable, last-mile, backhaul solution.
- The IEEE 802.17x standards address the Resilient Packet Ring which can handle multiple gigabit transmission speeds in opposite directions. This dual ring technology can be used in MAN and WAN networks.

4.5. **Network Design and Implementation:** Shall include levels of redundancy, fault tolerance, and disaster recovery based on budget unit business requirements. Network design and implementation shall be scalable and interoperable, as delineated herein, and documented in accordance with *Statewide Standard P800-S815, Configuration Management*.

- Budget unit requirements for business continuity and availability of services dictate the levels of redundancy, fault tolerance, and disaster recovery that are designed and implemented in networks.
- Scalable, interoperable network designs position budget units for incremental growth and expansion. A scalable, interoperable network design allows a budget unit to minimize the costs and disruptions of expansion while providing timely and responsive network changes when and where required.
- Scalable, interoperable network designs, incorporated with planning, ensure adequate network capacity, availability, and performance to meet changing business requirements including staffing levels, software applications, and facility addition, expansion, or relocation.
- *Statewide Standard P800-S815, Configuration Management*, recommends the use of a common, automated tool for design and documentation to allow for cross-agency analysis and opportunities for sharing and consolidation.

- 4.6. **Network Link Layer Access Protocol:** Shall be Ethernet, IEEE 802.3, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method.
- Ethernet is scalable, with current versions able to manage the increase of data flow and provide the bandwidth and “end-to-end” Quality of Service (QoS) necessary to support the requirements of multimedia and converged voice, data, and video applications.
 - The IEEE 802.3 Ethernet standards provide 10 / 100 / 1000 (1 Gbps) / 10,000 (10 Gbps) Mbps operation progressively providing higher bandwidth and improved performance.
 - The IEEE 802.3 standards provide an upgrade path resulting in a consistent management model across all operating speeds.
 - Full-duplex mode of Ethernet allows a simultaneous flow of network traffic from one workstation to another without collision issues.
 - The IEEE 802.3af PoE standard allows most IP platform devices requiring power to operate without supplemental AC power.
 - Network design, installation, and maintenance costs are minimized by preserving network architecture, management, software, and structured network cabling.
- 4.7. **Logical Network Topology:** Shall be a star or mesh, as appropriate, although the physical network topology may be a star, ring, or mesh.
- Star, ring, and mesh topologies are specified to minimize the effect of connection failures between devices while easing the addition or removal of network devices.
 - Star, ring, and mesh topologies are both scalable and flexible.
 - IEEE 802.3 Ethernet standards support star-wired Local Area Network (LAN) designs using point-to-point links and structured cabling topologies.
- 4.8. **Transport and Network Layer Protocols:** Shall be TCP/UDP and IP, respectively.
- TCP/UDP and IP make up an open, standards-based protocol suite that allows Internet access and the seamless integration of Intranets, Extranets, Virtual Private Networks (VPNs), and LANs.
 - IPv6 (Version 6) is the newest, accepted version of IP, which is designed as an evolutionary improvement from IPv4 (Version 4); however, IPv4 is acceptable for current deployment. IPv6 includes a transition mechanism designed to allow organizations to adopt and deploy IPv6 in an incremental, dispersed manner, while providing direct interoperability between IPv6 and IPv4 systems. IPv6 enhancements include QoS capabilities as well as the definition of extensions, which provide support for security authentication, data integrity, and confidentiality.
 - Dual stack IPv4-IPv6 network device architecture, IPv6 tunneling over Multi-Protocol Label Switching (MPLS) or IPv4, and IPv4 tunneling in a native IPv6 environment provide examples of transition mechanisms.

- TCP/UDP and IP protocols facilitate, simplify, and standardize the protocols used to deliver e-government services.
- 4.9. **Network Devices (routers, switches, firewalls, access servers, etc.):** Shall be securely deployed in accordance with applicable statewide IT security standards, and manageable with Network Management platforms that use the most currently approved, open, industry-standard versions³ of Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON).
- *Statewide Standard P800-S885, Physical Security*, addresses physically securing access to network devices, wiring closets, and other access points to provide security protection.
 - Backup-up generator power systems and/or Uninterruptible Power Supplies (UPS) protect network devices against loss of electrical power that could disrupt service delivery of mission-critical applications and converged services. Such devices shall be managed and network-connected to protect routers, LAN switches and VoIP/IPT systems. UPS systems should include Ethernet-based network management cards capable of SNMP monitoring via TCP/IP.
 - Environmental facilities (air conditioning, humidity controls, etc.) maintain acceptable operating ranges derived from applicable manufacturers' specifications.
 - SNMP and RMON facilitate the exchange of management information between network devices as well as network performance management, isolation and analysis of network problems, and growth planning.
 - SNMP is an Internet Engineering Task Force (IETF) standard defined by RFC 1157 and is part of the TCP/IP open-standards-based protocol suite recommended for the transport and network protocol layers.
 - Managed network devices help to ensure the continuous delivery of e-government services and internal budget unit business processes.
- 4.10. **Switching Technologies:** Shall be secure, in accordance with applicable statewide IT security standards, and used to achieve LAN network device connectivity in Open Systems Interconnection (OSI) Layers 2, 3, and 4. Switching devices shall comply with IEEE 802.1p/Q standards and IETF Multi-Protocol Label Switching (MPLS) to provide scalable, interoperable, IP quality of service (QoS).
- Switching enhances security and network management. It improves network performance by enabling the balancing of network traffic across multiple segments at wire-speed, thus reducing resource contention, providing for scalability, and increasing throughput capacity.
 - QoS features provide improved and more predictable network services by setting traffic priorities starting with the type of service (ToS) bits at Layer 2, then providing network traffic shaping, improved management, and congestion avoidance at Layer 3 with class of service (CoS)

³ For the purposes of this statewide standard, "most currently approved" assumes widespread mainstream adoption and implementation by industry.

categorization. Applying QoS globally within a network infrastructure reduces packet loss and improves performance characteristics.

- IP QoS enables networks to support existing and emerging multimedia service/application requirements. It enables application-aware networking, in which a network services its packets based on application information within the packet headers. IP QoS provides end-to-end service and policy-based control of a private and/or public IP network's performance.
- IEEE 802.1p enables network traffic prioritization and the seamless integration of data, voice, and video into converged services.
- IEEE 802.1Q trunking support enables segmentation of individual data, voice, and video client platform devices into separate logical virtual networks (VLANs). IEEE 802.1Q VLAN tagging uniquely identifies traffic from each VLAN, enabling traffic from multiple VLANs to share the same physical switch port link.
- MPLS is an IETF-specified framework that provides for designation, routing, forwarding, and switching of traffic flows through a network. MPLS interfaces with other IETF routing protocols such as Open Shortest Path First (OSPF).

4.11. **Routing Technologies:** Shall be open, industry-standards-based for Internet and inter-network connectivity. Routing technologies include the most currently approved versions of Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Integrated Intermediate System-to-Intermediate System (IS-IS), etc., and applicable multicast protocols including Internet Group Management Protocol (IGMP), Protocol Independent Multicast (PIM), Multiprotocol BGP (MBGP), etc. To avoid proprietary, single-source solutions, vendor-specific extensions to open, industry-standard, routing protocols used for budget unit inter-network connectivity shall be generally available for use and implementation by third-party manufacturers. Vendor-specific extensions should also be in planned draft or draft form submittal to the appropriate standards approval body.

- Routing protocols provide the information needed to quickly and efficiently direct incoming IP traffic to the correct destination.
- Routing technologies operate over a reliable transport protocol (TCP).
- Extensions to standards-based routing protocols provide for both IPv6 and IPv4.

4.12. **Converged Services:** Networks, including LAN, WLAN, MAN, WMAN, and WAN, shall accommodate secure connectivity, transmission, and the convergence of voice, video, and data application traffic. Secure transmission shall include VPN technology and encryption technologies, as necessary, as well as boundary and end-point security as described in *Statewide Standard P800-S830, Network Security*. To accomplish convergence, networks shall differentiate and service the different types of traffic based on application requirements. To avoid proprietary, single-source solutions, vendor-specific extensions to open, industry standards and protocols shall be generally available for use and implementation by third-party manufacturers. Vendor-specific

extensions should also be in planned draft or draft form submittal to the appropriate standards approval body.

- *Statewide Standard P800-S830, Network Security*, describes multi-layer protection, external connectivity to networks, both wire-based and wireless, as well as perimeter security technologies to provide for secure and seamless interconnection of communication networks and systems.
- *Statewide Standard P800-S850, Encryption Technologies*, describes minimum requirements for ensuring the authenticity, integrity, confidentiality, and reliability of digital information.
- IP QoS functions provide effective, policy-based control for differentiated traffic flows across a private and/or public network. Resilient Packet Ring (RPR) 802.17x, SONET, and Frame Relay QoS-to-IP internetworking provide end-to-end QoS in a mixed-link technology network.
- Ethernet QoS functions based on IEEE 802.1p standards and IETF RFC 2474/5 differentiated services (diffserv) architecture provide interoperability standards for network devices from multiple vendors.
- Diffserv facilitates end-to-end converged services by providing interoperability among multi-vendor environments through enabling the provisioning of differentiated levels of service across multiple, separate MANs, LANs, and WANs. Diffserv is scalable and deployable in the predominately “best-efforts” Internet. DiffServ is backwards compatible with IP Type of Service (ToS).
- Real Time Protocol (RTP), Real Time Control Protocol (RTCP), and Real Time Streaming Protocol (RTSP) transport and manage the real-time transmission of multimedia data over network services. RTP runs on top of User Datagram Protocol (UDP).
- Resource Reservation Protocol (RSVP) provides a means for reserving network resources to provide guaranteed network services, primarily bandwidth, to guarantee that applications transmitting end-to-end across networks and the Internet will perform at the desired speed and quality. RSVP requires support in all intermediate network devices to provide end-to-end transport guarantees.

4.13. **Converged Services Client Platform Devices**⁴: shall be capable of accepting and processing voice, video, and data applications within a single, secure, client platform device⁵ using the most currently approved versions of open, industry-standards for signaling protocols, compression, and media stream. Client platform devices shall accommodate the use of VLANs to segregate different types of network traffic, such as voice and data. To avoid proprietary, single-source solutions, vendor-specific extensions to open, industry standards and protocols utilized by client platform devices shall be generally available for use and implementation by third-party manufacturers. Vendor-specific extensions

⁴ Converged client platform device specifications and requirements will be further detailed in *Statewide Standard P720-S720, Platform Infrastructure*.

⁵ *Statewide Standard P720-S720, Platform Infrastructure*, addresses operating system security requirements of client platform devices.

should also be in planned draft or draft form submittal to the appropriate standards approval body.

- Signaling protocols include the most currently approved versions of Session Initiation Protocol (SIP) with Session Announcement Protocol (SAP) and Session Description Protocol (SDP), H.323, and Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) Protocol Q.931. SIP and H.323 use RTP to transport real-time transmission of multimedia data over network services.
- Standard compression/decompression (codec) techniques, with their respective mean opinion scores (MOS), include G.711 – 4.3 MOS, G.729 – 4.0 MOS, G.723 3.8 MOS.
- Transcoders are available to provide conversion between compression techniques such as G.711 to G.729 conversion.

- 4.14. **Inter-Network Transport Services:** Generally and commercially available transport services, commonly referred to as carrier services, shall incorporate open, secure, scalable, industry-standards-based, packetized services, such as Resilient Packet Ring (RPR) 802.17x, SONET, Frame Relay, etc., providing end-to-end QoS capable of transporting voice, video, and data applications within a converged media stream. TDM-based, dedicated transport services, such as T1 digital carrier, ISDN, etc., shall be acceptable only as a transitional strategy to fully-packetized inter-network transport services.
- Open, industry-standards-based networks allow for end-to-end QoS to be provisioned across multiple provider-based networks and internal networks to accommodate converged voice, video, and data applications.
 - Converged services provide cost-effective, efficient transport bandwidth utilization and management to deliver voice, video, and data applications.
- 4.15. **Internet-Based Virtual Network Services:** Shall be securely designed and implemented to include VPN technology as well as boundary and end-point security as described in *Statewide Standard P800-S830, Network Security*.
- Virtual network services utilize the Internet and are inherently scalable and interoperable.
 - Virtual network services utilizing VPN technologies securely provide a consistent, client-browser interface to authorized users⁶ and deliver enterprise-wide network and software application services regardless of location.
 - Virtual networks are an important business continuity element that allows continuation of mission-critical functions and services, regardless of location.
- 4.16. **VLAN Technologies:** Shall be implemented with converged network services to segregate different types of network traffic, such as voice and data, and as necessary to access applicable software applications.

⁶ An “authorized user” may be a software application system, a platform server, a service layer, or an individual user.

- VLANs are a logical group of network-attached devices on one or more LANs or LAN segments that are configured (using management software) to communicate as if the devices were attached to the same physical LAN segment or “wire.” The flexibility of VLANs is based on logical instead of physical connections.
- VLAN technology provides for the logical segmentation of a LAN into different broadcast domains to increase network performance in an environment with a high percentage of broadcasts and multicast traffic, the formation of virtual workgroups and simplified network administration.

4.17. **Network Interfaces:** Internal networks using “private,” unregistered Internet Protocol (IP) addresses for network workstations and appliances shall use reserved addresses as defined by the Internet Assigned Numbers Authority (IANA). Internal networks using “public,” registered IP addresses for network workstations and appliances are acceptable for current use. External networks communicating outside the budget unit shall use “public,” registered IP addresses for all external ports on internetworking devices.

- Network Address Translation (NAT) techniques deployed at network boundaries to external networks or the Internet enable the use of both registered and unregistered IP addresses while still providing the required connectivity to applications and the external network or Internet. NAT provides a firewall between the internal network and outside networks or the Internet by only allowing connections that originate inside the internal network.
- “Private,” unregistered IP addresses provide flexibility and simplify the process of adding workstations and devices to networks.
 - The 172.16.0.0 to 172.31.255.255 block of IP addresses is specifically reserved for IP telephony equipment and devices.
- The IANA has reserved three blocks of IP address space for “private” Internets (Network Working Group RFC 1918). The blocks are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255. Any IP addresses outside of these spaces lack coordination with IANA or an Internet registry when used as unregistered IP addresses.
- To prevent duplication and resulting loss of connectivity, the organization responsible for network administration of a budget unit shall coordinate all “private,” unregistered IP addresses within their domain of responsibility.
- “Public,” registered IP addresses provide the required uniqueness for Internet and network integrity.
- IANA provides coordination of all “public” IP address space.

4.18. **Internal Workstation Network IP Addresses:** Shall be assigned using Dynamic Host Configuration Protocol (DHCP). DHCP address allocation may be (1) an automatic allocation where DHCP assigns a permanent IP address to the workstation; (2) manually allocated and assigned by the DHCP

administrator; or (3) dynamically allocated where DHCP assigns an IP address to a workstation for a limited period of time (lease.)

- DHCP provides the flexibility needed for growth and migration of networks.
- DHCP facilitates and simplifies IP network administration and the addition of workstations and devices to networks.
- DHCP allows for central allocation and administration of IP addresses within a budget unit.

4.19. **Network Time Protocol:** Budget units shall use the Network Time Protocol (NTP) to securely obtain time information needed to synchronize network devices and computer clocks.

- NTP architecture and security models provide for operation in unicast and multicast modes, and include provisions for secure authentication using both symmetric key and public key cryptography.
 - NTP Version 4 includes provisions for an autonomous configuration capability, which provides for automatic server discovery and secure server authentication
- The official U.S. time public service is cooperatively provided by two time agencies: the National Institute of Standards and Technology (NIST) and the U. S. Naval Observatory (USNO).
- Atomic Clock accuracy is also available using satellite navigation technology or the radio station WWVB Atomic Clock time signal transmitted from Colorado. Radio or Global Positioning System (GPS) atomic clock services provide accurate time behind a firewall maintaining budget unit security.
- Additionally, time information is available from Arizona Department of Administration (ADOA), Information Security Services.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the Glossary of Terms located on the GITA website for definitions and abbreviations.

6. REFERENCES

- 6.1. A. R. S. § 41-621 et seq., “Purchase of Insurance; coverage; limitations, exclusions; definitions.”
- 6.2. A. R. S. § 41-1335 ((A (6 & 7))), “State Agency Information.”
- 6.3. A. R. S. § 41-1339 (A), “Depository of State Archives.”
- 6.4. A. R. S. § 41-1461, “Definitions.”
- 6.5. A. R. S. § 41-1463, “Discrimination; unlawful practices; definition”.
- 6.6. A. R. S. § 41-1492 et seq., “Prohibition of Discrimination by Public Entities.”
- 6.7. A. R. S. § 41-2501 et seq., “Arizona Procurement Codes, Applicability.”
- 6.8. A. R. S. § 41-3501, “Definitions.”
- 6.9. A. R. S. § 41-3504, “Powers and Duties of the Agency.”
- 6.10. A. R. S. § 41-3521, “Information Technology Authorization Committee; members; terms; duties; compensation; definition.”

- 6.11. A. R. S. § 44-7041, “Governmental Electronic Records.”
- 6.12. Arizona Administrative Code, Title 2, Chapter 7, “Department of Administration Finance Division, Purchasing Office.”
- 6.13. Arizona Administrative Code, Title 2, Chapter 10, “Department of Administration Risk Management Section.”
- 6.14. Arizona Administrative Code, Title 2, Chapter 18, “Government Information Technology Agency.”
- 6.15. State of Arizona Target Network Architecture.
- 6.16. Statewide Policy P100, Information Technology.
- 6.17. Statewide Policy P700, Enterprise Architecture.
- 6.18. Statewide Policy P710, Network Architecture.
- 6.19. Statewide Policy P800, IT Security.
- 6.20. Statewide Standard P100-S102, Platform Infrastructure.
- 6.21. Statewide Standard P800-S815, Configuration Management.
- 6.22. Statewide Standard P800-S830, Network Security.
- 6.23. Statewide Standard P800-S850, Encryption Technologies.
- 6.24. Statewide Standard P800-S885, Physical Security.

7. ATTACHMENTS

None.