

**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**

The purpose of this standard is to coordinate budget unit and State implementations of target platform infrastructure(s). This standard promotes the implementation of platforms that incorporate open systems architecture and proven, pervasive, or industry-wide standards. It has been developed in support of the fair competition laws of Arizona, A.R.S. § 41-2565, by providing a range of target platforms throughout the product lifecycle.

**3. SCOPE**

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization 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 or 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**

The term “platform” applies to servers, storage, and end-user (client) devices with their respective operating systems, interfaces, and drivers that provide a framework for interoperability, scalability, and portability. Open systems architecture for platforms will further promote the sharing of information/data and other IT resources in support of e-government initiatives and programs.

Attachment A, Target Platform Architecture Assessment, identifies requirements for versatility, operating systems, security, and open standard interfaces / drivers that are critical to platform technologies. The State of Arizona “As-Is” Platform Assessment, available at [http://www.azgita.gov/enterprise\\_architecture/](http://www.azgita.gov/enterprise_architecture/) depicts the platforms installed throughout state agencies, as reviewed by CIO Council and approved by the State CIO.

Target platform architecture must incorporate a range or requirements since at any point in time, given the dynamic nature of the information technology industry and platform-product life cycles, a particular target platform device may no longer

completely comply with all requirements. This approach allows budget units to maximize their current investment in certain devices and services, as well as to develop a transition plan to allow obsolete or non-conforming platform elements to be phased out. The intent of the following standards is to specify requirements while allowing a reasonable scoring range, using the assessment tool, for target platform compliance.

- 4.1. VERSATILITY: The device shall be flexible, adaptable, and scalable to support interoperability and provide for new and expanding service requirements.
  - Capability shall exist for achieving related architecture targets without requiring major upgrades and additional costs.
  - Capability shall exist for delivering and/or providing secure (as defined in [Statewide Policy P800, IT Security](#) and related standards documents) end-user interface access to a variety of business applications without necessitating substantial modifications, regardless of end-user location.
    - Applications include, but are not limited to, e-mail, human resources information systems (HRIS), financial management systems (FMS), Internet, office productivity software, telephony, and voice mail.
  - Capability shall exist for delivering and/or providing end-user interface access to a wide variety of business applications using a fully converged network, regardless of end-user location.
  - Target Network Architecture standards shall be maximized in the connectivity of devices.
  - The device shall be scalable, without substantial modification, to allow for increased demands for services and new applications.
  - Widespread choices for off-the-shelf application solutions, without modifications, shall be available for the device.
  - The versatility of the device shall directly improve the quality and timeliness of budget unit business functions.
- 4.2. OPERATING SYSTEM: The device shall utilize either an open, industry-standard, secure operating system or a pervasive, industry-standard, secure operating system.
  - The open or industry de-facto standard operating system currently installed shall be available for all similar devices offered by the manufacturer.
  - The operating system shall provide for updates to be pushed to, or accepted by, all associated devices.
  - The device shall be capable of efficiently running the most current production operating system recommended by the manufacturer; the version installed shall be no more than one major revision behind the most current available version.
  - Future production releases of the operating system shall be scheduled by the manufacturer at the time of implementation.
- 4.3. OPERATING SYSTEM SECURITY: The device shall have an appropriate, as determined by the budget unit with regard to [Statewide Policy P800, IT](#)

[Security](#) and related Statewide IT security standards, level of security functionality incorporated as part of the installed operating system.

- Operating system security services, including network connectivity and access, authentication and authorization techniques, session controls, and encryption technologies shall adhere to Statewide IT security standards.
- Logging and security controls for applications, platform, and network levels shall be integrated to eliminate, or at least reduce, redundancies.
- Support for integrated LDAP-based directory services shall be available.
- Disabling of security options shall be prevented at the user level.
- Security updates from the operating system shall be capable of being pushed to, or accepted by, all associated devices.
- Logging and restriction (including prevention of end-user override) of particular functions and services shall be enabled, including:
  - Non-essential or redundant services,
  - Any communication options susceptible to or prone to abuse, and
  - Utilities at the operating system level.
- Removals of extraneous services, open ports, etc., shall be enabled from default installations of the operating system, and prevented from returning during subsequent upgrades.
- Budget units shall document procedures to routinely review installed platform device(s) operating system security services.

4.4. INTERFACES: The device shall be capable of adhering to applicable, open-system-standard, interface specifications.

- Open-systems standards for any particular interface shall be available and in use.
- Management using standard SNMP-based management tools shall be enabled.
- Network communication protocols shall adhere to [Statewide Standard P710-S710, Network Infrastructure](#).
- Off-the-shelf devices and peripherals conforming to open-systems standards shall be readily obtainable.

4.5. DRIVERS: The device shall be capable of utilizing input/output (I/O) drivers that incorporate IEEE-standard interfacing and industry de-facto standard software drivers.

- Multiple peripheral devices using open-standard drivers shall be available.
- Off-the-shelf peripherals that conform to open system standards shall be readily available.

4.6. SHARED PLATFORM DEVICES (MAINFRAMES, SERVERS, STORAGE, etc.): These are critical components of the State's IT infrastructure providing reliable and pervasive availability of, access interfaces with, and processing for, the State's distributed information processing environment.

- 4.6.1. Shared platform devices shall be securely deployed in accordance with statewide IT security standards.

- Statewide Standard P800-S885, IT Physical Security, addresses physically securing access to shared platform devices, network devices, wiring closets, and other access points to provide security protection.
  - Shared platform devices supporting mission-critical applications and converged services should be configured and deployed with sufficient reliability, redundancy, and fault tolerance to permit continued operations in accordance with Statewide Standard P800-S865, IT Disaster Recovery Planning (DRP).
  - Uninterruptible Power Supplies (UPS) protect shared platform devices against loss of electrical power that could disrupt service delivery of mission-critical applications and converged services. UPS facilities should be network-connected and manageable in accordance with Statewide Standard P800-S830, Network Security.
  - Environmental facilities (air conditioning, humidity controls, etc.) maintain acceptable operating ranges derived from applicable manufacturers' specifications.
- 4.6.2. Access to shared platform devices shall be controlled to prevent unauthorized access, both internal and external, in accordance with Statewide Standard P800-S830, Network Security.
- 4.6.3. Within the parameters contained in this standard, target technologies as identified in the Arizona Enterprise Architecture Target Technology Table, and unique software application requirements, budget units should standardize shared platform devices and associated operating systems to increase integration and reduce acquisition and support costs. Standardization of shared platform devices provides a common infrastructure for virtual or physical consolidation, shared reusable services, as well as web-services-based e-government software applications.
- 4.6.4. Management tools for shared platform devices, if utilized by a budget unit, shall be standardized within the budget unit and shall be Simple Network Management Protocol (SNMP) compatible to provide for remote management of devices and the exchange of management information between platform and network devices. Budget units should consider the consolidation/integration of device management, provisioning, configuration control, patch management, etc., into a single toolset.
- 4.6.5. Hardcopy and electronic documentation of shared platform device configurations, access lists, diagrams, etc., shall be destroyed, as appropriate, when superseded, or no longer needed.
- 4.7. **PATCH MANAGEMENT**: Budget units shall develop and implement written procedures that identify roles and responsibilities for implementing patch management that include the following activities:

- 4.7.1. Designated budget unit employees or contractors shall proactively monitor for operating system patches for all platform devices attached to their network by ensuring that applicable patches are correctly acquired, tested, and installed in a timely manner. IT device manufacturers, security organizations, security vendors, and the Arizona Department of Administration (ADOA) Statewide Infrastructure Protection Center (SIPC) provide various tools and services to assist in identifying vulnerabilities and respective patches.
  - 4.7.2. Where practical and feasible, budget units shall test patches in a test environment prior to installing the patch. Testing exposes detrimental impacts to internal/external enterprise-wide application software systems, community-of-interest application software systems, and other third-party application software systems.
  - 4.7.3. Budget units shall query SIPC prior to installing patches in production to determine if other State budget units have experienced problems during testing or post-installation. Budget units shall report testing and production problems discovered with patches to SIPC.
  - 4.7.4. Patches shall be installed (use of an automated tool is recommended) on all affected platform devices. Designated employees or contractors shall monitor the status of patches once they are installed.
  - 4.7.5. Patches make software changes to the configuration of a platform device and shall be controlled and documented in accordance with Statewide Standard P800-S815, Configuration Management.
- 4.8. END-USER PLATFORM DEVICE CONFIGURATIONS: Within the parameters contained in this standard and target technologies as identified in the Arizona Enterprise Architecture Target Technology Table, budget units should determine and control uniform, standard configurations for end-user platform devices and associated operating systems to maximize interoperability, portability, and economies of scale, while simplifying installation, upgrades, support, and maintenance issues. Standard configurations should consider existing budget unit software applications and statewide enterprise software applications, as well as web-services-based e-government software applications.
- 4.9. CONVERGED SERVICES END-USER PLATFORM DEVICES: Devices capable of accepting and processing voice, video, and data applications within a single, secure, end-user platform device shall:
- Use the most currently approved versions of open, industry-standards for signaling protocols, compression, and media stream.
    - Signaling protocols, compression, and media stream are defined in Statewide Standard P710-S710, Network Infrastructure.
    - To avoid proprietary, single-source solutions, vendor-specific extensions to open, industry standards and protocols utilized by end-user platform devices 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.
  - Accommodate the use of separate logical virtual networks (VLANs) to segregate different types of network traffic, such as voice and data.
  - Conform to IEEE 802.3af Power over Ethernet Standard if receiving AC power over Ethernet.
- 4.10. PORTABLE PLATFORM DEVICES: Portable platform devices (laptops, PDA's, USB Flash/Thumb drives, memory sticks, external hard drives, etc.) with the capability to execute software applications, and/or store information (documents, databases, etc.) and connect to budget unit networks and the Internet:
- Shall adhere to authentication requirements as defined by Statewide Standard P800-S820, Authentication and Directory Services, connectivity and security requirements as defined by Statewide Standard P800-S830, Network Security, as well as all other applicable Statewide IT security standards;
  - Shall disable any automatic logon capability;
  - Should secure the operating system file system through the use of Access Control Lists (ACLs) or an equivalent method;
  - Should, if applicable, secure the platform device with a cable locking system or lockdown enclosure;
  - Should consider the use of anti-theft PC cards; and
  - Should encrypt critical files.
- 4.11 PORTABLE MEDIA DEVICES: Are usually handheld multimedia (sound, images, video) devices such as MP3 Players, iPods, DVD Players, Smart/Hybrid Phones etc., which can play digital music, store and display, images (GIFs and JPEGs), and display movie files that have been downloaded from the Internet or stored on a personal computer. Such devices can provide a valuable delivery channel for distributing and communicating information to state employees on budget unit programs and services, for orientation and training, for statewide initiatives, for security awareness and training, and a host of other communiqué important to the state. It is the responsibility of the budget unit CIO to decide whether personal media devices from state employees can be used on state client devices or whether they should be state issued.
- 4.12 END POINT SECURITY: End-user platform devices, including State-owned assets, end-user devices used by remote workers and telecommuters, as well as third-party entities, connected to the budget unit's internal network should be securely protected in accordance with Statewide Standard P800-S830, Network Security.
- 4.13 CONFIGURATION MANAGEMENT: Platform devices (assets) shall be controlled, inventoried, and managed in accordance with P800-S815, Configuration Management.

- 4.14 “AS-IS” PLATFORM ASSESSMENT RATINGS: Given the dynamic nature of target platform lifecycles and advances in the information technology industry, changes to the Arizona “As-Is” Platform Assessment table are inevitable.
- When an budget unit plans to implement a platform not included on the current Arizona “As-Is” Platform Assessment table<sup>1</sup> but considered to be an open, industry standard or de-facto industry standard, the CIO shall submit a Target Platform Architecture Assessment (Attachment A) to GITA either in advance of or concurrent with the Project Investment Justification (PIJ).
  - Requests for changes to platform ratings shall come from budget unit CIOs via submittal to GITA of a completed Target Platform Architecture Assessment (Attachment A) for the item requiring change.
  - Arizona’s State CIO in conjunction with the CIO Council shall have final approval of all platform assessment ratings, whether conducted virtually or at a CIO Council meeting.

## 5 DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the GITA website at [http://www.azgita.gov/policies\\_standards/](http://www.azgita.gov/policies_standards/) 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 Code, Applicability.”
- 6.8. A. R. S. § 41-2565, “Specifications, Maximum Practicable Competition.”
- 6.9. A. R. S. § 41-3501, “Definitions.”
- 6.10. A. R. S. § 41-3504, “Powers and Duties of the Agency.”
- 6.11. A. R. S. § 41-3521, “Information Technology Authorization Committee; members; terms; duties; compensation; definition.”
- 6.12. A. R. S. § 44-7041, “Governmental Electronic Records.”
- 6.13. Arizona Administrative Code, Title 2, Chapter 7, “Department of Administration Finance Division, Purchasing Office.”
- 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 Platform Architecture.
- 6.16. [Statewide Policy P100, Information Technology.](#)

---

<sup>1</sup> The Arizona “As-Is” Platform Assessment table is available at:  
[http://www.azgita.gov/enterprise\\_architecture/NEW/Platform\\_Arch/platform\\_assess.htm](http://www.azgita.gov/enterprise_architecture/NEW/Platform_Arch/platform_assess.htm).

- 6.17. [Statewide Policy P720-S720, Platform Architecture.](#)
  - 6.18. [Statewide Policy P800, IT Security.](#)
    - 6.18.1 [Statewide Standard P800-S815, Configuration Management.](#)
    - 6.18.2 [Statewide Standard P800-S820, Authentication and Directory Services.](#)
    - 6.18.3 [Statewide Standard P800-S830, Network Security.](#)
    - 6.18.4 [Statewide Standard P800-S865, IT Disaster Recovery Planning \(DRP\).](#)
    - 6.18.5 [Statewide Standard P800-S885, IT Physical Security.](#)
  - 6.19. [Statewide Standard P710-S710, Network Infrastructure.](#)
- 7. ATTACHMENTS**  
Attachment A – “Target Platform Architecture Assessment”

**ATTACHMENT A. TARGET PLATFORM ARCHITECTURE ASSESSMENT.**

This assessment is designed to support the planning and implementation of Target Platform Architecture recommended standards and best practices. The assessment applies to IT projects that include business requirements that propose or require modifications and/or additions to existing deployments of platform devices.

**Score.** Questions for the four (4) platform device categories are scored with one (1) point for a “Yes” answer, and zero (0) for a “No” answer. Maximum possible is the total number of questions for each category.

**Definitions:**

**Applicable** is defined as pertinent, related to, relevant, and appropriate.

**Capability** is the potential and ability for development or use. It is the capacity to be used or developed for a purpose.

**Device** includes logical groupings or categories of server, storage, and end-user (client) platforms in use statewide, or within a budget unit.

**Maximize** is defined as taking full advantage of the subject attribute(s).

**Variety** is defined simply as more than one. Note: the intent of versatility is to maximize flexibility and usefulness of a device relative to the applicable budget unit business applications.

**Widespread** is defined as extensive and prevalent.

**Platform Device Name/Description:**

Category	Max. Possible	Score	Category Description
1. Versatility	8		Provides interoperability, flexibility, adaptability, and scalability without requiring substantial modification.
2. Operating Systems	6		Utilizes open- or pervasive-industry-standard, secure, operating systems.
3. Operating Systems Security	7		Addresses the security functionality of Operating Systems.
4. Open Standard Interfaces & Drivers	4		Adheres to open-system-standard interface specifications and utilizes device drivers with IEEE interfacing and industry de facto standard protocols and formats.
<b>Total Rating Points</b>	25		

**1. Versatility** refers to a device’s capability (assuming connectivity where applicable) to provide interoperability, flexibility, adaptability, and scalability without requiring substantial modification.

Score 1 Rating Point for a “Yes” answer	Yes
1. Is the device capable of delivering applicable EA Target Technologies and Statewide IT standards without major upgrades and additional costs?	
2. Is the device capable of delivering or providing secure (as defined by Statewide IT Security Policy and Standards) end-user interface access to a variety of business applications (HRIS, email, office productivity applications, Internet, telephony, voice mail, etc.) without substantial modifications, regardless of end-user location?	
3. Is the device capable of delivering or providing end-user interface access to a variety of business applications maximizing a fully converged network, regardless of end-user location?	
4a. Server only – is the device capable of hosting or delivering multiple, and varied application solutions, with sufficient reliability, redundancy, and fault tolerance to support essential budget unit business operations?	
4b. Storage only – is the device capable of hosting or delivering storage for multiple, and varied application solutions, with sufficient reliability, redundancy, and fault tolerance to support essential budget unit business operations?	
4c. End-user device only – is the device capable of providing one common point for end-user connectivity access and productivity for multiple and varied application solutions?	
5. Is the device able to maximize the use of the Statewide Network Infrastructure standards?	
6. Is the device capable of accommodating increased demands for service and new application solutions without substantial modifications?	

7. Are widespread choices for off-the-shelf application solutions, without modifications, available for this device?	
8. Does the versatility of this device directly improve the quality and timeliness of budget unit business functions?	
<b>Total Rating Points</b>	

**2. Operating Systems** refer to a device's, or networks, capability to utilize open- or pervasive-industry-standard operating systems.

Score 1 Rating Point for a "Yes" answer	Yes
1. Is an open-industry-standard operating system currently available for this device?	
2. Is the operating system currently deployed with this device an open or industry de facto standard operating system?	
3. Does the operating system currently deployed with this device allow for all updates to be pushed to, or accepted by, all associated devices?	
4. Does the same version of the operating system currently deployed with this device have mass availability?	
5. Is the installed version of the operating system currently deployed with this device the most current production version, or undergoing continued development by the manufacturer?	
6. Is the operating system currently deployed with this device scheduled for future production releases?	
<b>Total Rating Points</b>	

**3. Operating Systems Security** refers to a security functionality that is available with the Operating System (must be answered relative to responses in 2. Operating Systems.)

Score 1 Rating Point for a "Yes" answer	Yes
1. Do the operating system security services align with Statewide IT Security Policy and Standards?	
2. Does the operating system security allow for logging and the security controls for applications, platform, and network levels to be integrated to reduce and eliminate redundancies?	
3. Does the operating system support access, authentication, and authorization techniques as defined in the Statewide IT Security Policy and Standards?	
4. Does the operating system allow for an integrated LDAP directory service?	
5. Does the operating system allow for all security updates to be pushed to, or accepted by, all associated devices?	
6. Does the operating system allow for logging and the restriction, including preventing end-user override, of particular functions or services, such as non-essential or redundant services, communication options that are susceptible or prone to abuse, and operating-system-level utilities?	
7. Can extraneous services, open ports, etc., be easily removed from "default installations of the operating system" and prevented from returning when the operating system is upgraded?	
<b>Total Rating Points</b>	

**4. Open Standard Interfaces and Drivers** refer to a device's capability to adhere to open-system-standard interface specifications and to utilize device drivers that use IEEE and industry de facto standard protocols and formats.

Score 1 Rating Point for a "Yes" answer	Yes
1. Does the device utilize Statewide Network Infrastructure Standards for communication protocols?	
2. Is the device capable of being configured, managed, and maintained using standard SNMP-based management tools?	
3. Is the device capable of utilizing open-standard drivers that employ IEEE-interfaces and industry de facto standard software drivers?	
4. Are multiple, off-the-shelf, peripheral devices that conform to open-system-standards and that utilize industry de facto standard drivers available for this device?	
<b>Total Rating Points</b>	