


<p>ARIZONA STATEWIDE SECURITY STANDARD</p>	<p>STATEWIDE STANDARD</p>	 <p>State of Arizona</p>
--	-------------------------------	--

STANDARD: System and Communication Protection

DOCUMENT NUMBER:	S8350
EFFECTIVE DATE:	JULY 1, 2015
REV:	DRAFT

1. AUTHORITY

The authority for this standard is based on Arizona Revised Statutes (A.R.S.) 41-3504: Powers and duties of the department. The Arizona Department of Administration (ADOA) develops, implements, and maintains a coordinated statewide plan for information technology. This includes adopting statewide technical, coordination and security standards for information technology. (A.R.S.)§ 18-104 and § 18-105.

2. PURPOSE

The purpose of this standard is to provide additional specificity to the associated policy requirements.

3. SCOPE

Application to Budget Units - This standard applies to all Budget Units (BUs). A BU 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 or judicial branches. A.R.S. § 18-101(1).

3.1 Application to Systems – The standard applies to all state information systems.

Categorization of systems is defined within the Information Security Program Policy.

- a. **(P)Policy statements preceded by “(P)” are required for state information systems categorized as Protected.**
- b. **(P-PCI) Policy statements preceded by “(P-PCI)” are required for state information systems with payment card industry data (e.g., cardholder data).**
- c. **(P-PHI) Policy statements preceded by “(P-PHI)” are required for state information systems with protected healthcare information..**

- d. **(P-FTI) Policy statements preceded by “(P-FTI)” are required for state information systems with federal taxpayer information.**

4. EXCEPTIONS

None.

5. ROLES AND RESPONSIBILITIES

Refer to associated Policy (P8350 – System and Communication Protection Policy).

6. STATEWIDE POLICY

- 6.1 **(P) Implement DMZ** – The BU shall ensure the state information system prohibits direct public access between the Internet and any system component in the Protected state information system. The DMZ shall: [PCI DSS 1.3]
 - a. **Limits inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; [PCI DSS 1.3.1]**
 - b. **Limits inbound Internet traffic to IP addresses within the DMZ; [PCI DSS 1.3.2]**
 - c. **Does not allow any direct connections inbound or outbound for traffic between the Internet and the Protected state information system; [PCI DSS 1.3.3]**
 - d. **Does not allow internal addresses to pass from the Internet into the DMZ; [PCI DSS 1.3.4]**
 - e. **Does not allow unauthorized outbound traffic from the Protected state information system to the Internet; [PCI DSS 1.3.5]**
 - f. **Implements stateful inspection, also known as dynamic packet filtering (i.e., only established connections are allowed into the network); [PCI DSS 1.3.6]**
 - g. **Places system components that store Confidential data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks; and [PCI DSS 1.3.7]**
 - h. **Does not disclose private IP addresses and routing information to unauthorized parties (Note: methods to obscure IP addressing may include: NAT, placing servers behind proxy servers, removal route advertisements for private networks that employ registered addressing, or internal use of RFC 1918 address space instead of registered addresses). [PCI DSS 1.3.8]**
- 6.2 **(P) Firewall Configuration** – The BU shall build firewall and router configurations that restrict connections between Non-Protected systems (Standard state information

systems or untrusted networks) and any system components in the Protected state information system. The configurations shall: [PCI DSS 1.2]

- a. **Restrict inbound and outbound traffic to that which is necessary for the Protected state information system; [PCI DSS 1.2.1]**
- b. **Secure and synchronize router configuration files; and [PCI DSS 1.2.2]**
- c. **Implement perimeter firewalls between any wireless networks and the Protected state information system, and these firewalls are configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the Protected state information system. [PCI DSS 1.2.3]**

6.3 Acceptable Encryption Algorithms – The following encryption algorithms are considered acceptable for use in state information systems to protect the transmission or storage of Confidential information and Protected system access.

6.3.1 (P) Acceptable Security Strength – the security strength of an encryption algorithm is a projection of the time frame during which the algorithm and the key length can be expected to provide adequate security. The security strength of encryption algorithms is measured in bits, a measure of the difficulty of discovering the key.

- a. **The current minimum key strength for Protected state information systems and Confidential data is 112 bits.**

6.3.2 Symmetric Encryption Algorithms – The following symmetric encryption algorithms are considered acceptable for use in state information systems.

Algorithm	Reference	Acceptable Key Strengths
Advanced Encryption Standard (AES)	FIPS 197	128, 192, or 256 bits
Triple Data Encryption Algorithm (TDEA) (three key 3DES)	SP 800-67	168 bits

6.3.3 Key Agreement Schemes – The following key agreement schemes are considered acceptable for use in state information systems.

Key Agreement Scheme	Reference	Acceptable Key Strengths	
		Finite Fields	Elliptical Curves
Diffie-Hellman (DH) or MQV	SP 800-56A	P = 2048	N: 224-255 and H=14
	SP 800-	Q= 224 or 256	N: 256-383 and H=16

	135		N: 384-511 and H=24 N: 512+ and H=32
RSA-based	SP 800-131A	N = 2048	

6.3.4 Hash Functions – The following hash functions are considered acceptable for use in state information systems.

Digital Signature Generation	Digital Signature Verification	Non-digital signature generation applications
SHA-224	SHA-224	SHA-1
SHA-256	SHA-256	SHA-224
SHA-384	SHA-384	SHA-256
SHA-512	SHA-512	SHA-384 SHA-512

6.3.5 Digital Signature Algorithms – The following digital signature algorithms are considered acceptable for use in state information systems.

Digital Signature Algorithm	FIPS Publication	Digital Signature Generation Settings	Digital Signature Verification Settings	Relative Strength
Digital Signature Standard (DSA)	FIPS 186-4	p >= 2048, q = 224	p >= 2048, q = 224	>= 112 bits
RSA Digital Signature	FIPS 186-4	2048	2048	>= 112 bits
ECDSA	FIPS 186-4	224	224	>= 112 bits

6.3.6 Message Authentication Codes – The following message authentication codes are considered acceptable for use in state information systems.

Hash Algorithms	Hash Generation	Hash Verification
HMAC	>=112 bits	>=112 bits

CMAC	AES, 3DES	AES, 3DES
CCM and GCM/GMAC	AES	AES

7. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the ADOA website.

8. REFERENCES

- 8.1 Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), NIST Special Publication 800-56A, March 2007
- 8.2 Recommendations for the Triple Data Encryption Algorithm (TDEA) Block Cipher (Revised), NIST Special Publication 800-67, January 2012
- 8.3 Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST Special Publication 800-131A, January 2011.
- 8.4 Recommendations for Existing Application-Specific Key Derivation Functions, Revision 1, NIST Special Publication 800-135, December 2011
- 8.5 Digital Signature Standard (DSS), Federal Information Processing Standards Publication, FIPS PUB 186-4, July 2013
- 8.6 Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication, FIPS PUB 197, November 2001

9. ATTACHMENTS

NONE