STATE of ARIZONA

Government Information Technology Agency	**Statewide STANDARD**	**TITLE: Encryption Technologies**
	P800 – S850 Rev 3.0	**Effective Date: May 7, 2008**

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (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)))). The Statewide Information Security and Privacy Office shall serve as the strategic planning, facilitation and coordination office for information technology security in the state (A.R.S. § 41-3507(A)).

2. PURPOSE

This standard establishes acceptable criteria for the use of encryption technologies for securing confidential[1] data/information to mitigate information risks for the State of Arizona. As a custodian of public and confidential information, the state must further protect private and sensitive data/information from all cyber threats[2] and vulnerabilities[3] whether external or internal to the state.

3. SCOPE

This applies to all budget units. 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 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

Encryption technologies protect confidential information[1] during transmission over state networks and in storage by using algorithms and a key mechanism which renders information unreadable for unauthorized intruders on state systems. The information is mathematically protected against disclosure and cannot be read by someone who does not have a corresponding key to decrypt the information. Encryption is a defense-in-depth strategy for the protection of informational assets of the state.

---

[1] S741 Classification and Categorization of Data Standard, Section 4.1 Confidential Data/Information is personal/private information and other information considered sensitive to the State.

[2] Cyber Threats are considered cyber attacks/crimes and terrorism activities that may compromise electronic state services and/or operational services, or portions thereof for state government.

[3] Vulnerabilities are where state production/control systems may be exposed to cyber attacks from either outside or inside the control system that can affect communication networks, operating systems, application systems, and data/information.

Therefore, all Budget Units shall deploy the use of encryption and protection techniques as listed below for the transmission of confidential data/information over state networks and as final repository in technology storage devices.

4.1 **TRANSMISSION ENCRYPTION TECHNOLOGIES**

All Budget Unit networks and security protocols shall deploy and support, at a minimum, either Triple DES (TDES) or Advanced Encryption Standard (AES) for the transmission of confidential data/information. Budget Units with deployments other than TDES or AES, are grand-fathered for a period of three years from an effective date of April 2, 2008. This requirement will aid in providing a trusted computing-base for encryption services that is essential for maintaining confidentiality, integrity, and non-repudiation of confidential information across state networks. Protection methods[4] listed below shall also be considered and used for additional protection of state networks:

4.1.1 IPSEC– a suite of authentication and encryption protocols suitable for all types of Internet Protocol (IP) traffic that is used to create virtual private networks (VPN). IPSEC allows confidential information to be sent securely between two end-stations or networks over an un-trusted communications medium. This should be considered as a technology for securing Internet and other IP communications in connecting authorized external customers at defined locations;

4.1.2 Secure Shell (SSH) – may be deployed solely for the remote administration of confidential data/information and their systems;

4.1.3 Secure Sockets Layer (SSL) – the secure sockets layer specification may be deployed to provide secured access to confidential data/information on Web servers. When SSL is used to protect Budget Unit confidential information, the most current version shall be used with 128-bit encryption;

4.1.4 Virtual Private Networks (VPN) – should be deployed in environments where data-link-layer encryption is not a practical solution to maintain and operate. VPN technology using IPSEC encryption can be implemented independently from a particular link-layer communications technology (e.g., HDLC, Frame Relay, FDDI, Ethernet, Gigabit Ethernet, ATM, etc.) As such, this standard strongly encourages the use of VPN technology to secure confidential communications;

4.1.5 Data-Link (symmetrical) Encryption – may be used in environments where Virtual Private Network management would not be a reasonable encryption implementation to maintain and operate and where use and management of VPN technology would not be warranted;

4.1.6 Secure /Multipurpose Internet Email Extension (S/MIME) – like PGP, S/MIME is a standards-based security enhancement to secure email and

[4] S830 Network Security Standard

message attachments that provides strong authentication through digital signatures, message confidentiality, integrity and non-repudiation.

4.1.7 Pretty Good Privacy (PGP) – may be used to protect sensitive information, transmitted via e-mail, using a minimum key-size of 2048 bits. Public key information may be maintained on public or internal PGP key servers. Please refer to Secretary of State's PGP policy at http://www.azsos.gov/pa/PGP-CP.pdf

4.1.8 Public Key Infrastructure (PKI) – recommended PKI-based technical functionality is defined by Standard X.509 and its extensions, in the evolving definition developed by the Internet Engineering Task Force (IETF), through the PKIX Standards Development Task Group. This standard provides and defines certified identification of digital signatures having integrity, nonrepudiation, and authentication. Please refer to Secretary of State's PKI policy and procedures at http://www.azsos.gov/pa/

4.1.9 All Budget Units shall coordinate PGP and PKI electronic signature-related projects and implementations with the Office of Secretary of State which has statutory and policy authority for electronic signatures (A.R.S. § 41-132 Electronic and Digital Signatures).

4.2 **STORAGE ENCRYPTION TECHNOLOGIES**: All confidential data/information residing on Direct Attached Storage (DAS) devices, Network Attached Storage (NAS) devices, and Storage Area Network (SAN)[5] devices, and all portable devices[6], shall be encrypted and compatible with communications and security protocols as identified in *Statewide Standard P700-S710, Network Infrastructure* and *Statewide Standard P800-S830, Network Security*. Encryption technologies shall also be compatible with state platform[7] operating systems. All Budget Units shall determine its encryption requirements and deploy at least one or more encryption methods listed below for the protection of confidential data/information:

4.2.1 Full-Disk Encryption – encrypts all data on a hard drive for a client device. This includes the entire operating system, all applications, and all data/information. Full-disk encryption software contains components that are independent of the operating system and execute before the operating system is loaded as well as authentication. The system is rendered unintelligible and unusable in the event of a cyber crime or terrorism.

Full-Disk Encryption should have the following capabilities: Pre-boot authentication for laptops/table PC's; file and folder-based encryption capabilities built into the operating system; supports single Sign-On; remote install capability; supports multiple algorithms and has the

[5] P720 Platform Architecture Policy on storage devices.
[6] S720 Platform Infrastructure Standard on portable devices.
[7] The term "platform" applies to servers, storage, and end-user (client) devices, including portable devices, with respective operating systems, interfaces, and drivers that provide a framework for interoperability, scalability, and portability.

ability to disable supported and unsupported algorithms in the event of conflict.

4.2.2 File (Folder) Encryption – provides encryption for specific files or folders. File-encryption solutions provide automatic security since each new file/folder encryption capability must be manually turned off/on.

File (Folder) Encryption should have the following capabilities: Must be able to support all state operating systems, all applications and related software programs in addition to productivity software[8] for the state; ability to support a multitude of server(s) and file systems; provide simple recovery mechanisms for the recovery of lost keys of encrypted files/folders; integrate seamlessly with mobile email; supports security concepts and methods of "separation of duties".

4.2.3 Back-up and Archive Media Encryption – provides benefits not only for protecting data in storage but also in the disposal of backup media. Many privacy regulations include disposal of back-up and archive media, while disclosure regulations generally dictate a retention period for back-up and archive data. Without encryption, media disposal is difficult; therefore, many entities keep back-up and archive media longer than needed or legally prudent. By deleting the encryption key, media is rendered unreadable. With a rotating key sequence, a regular pattern of retention and disposal can be automatically enforced.

Back-up and Archive Media Encryption should have the following capabilities: Integrates seamlessly into the backup process and devices; offers flexible options for data restoration and disaster recovery and supports various backup media types used by the state.

4.2.4 Mass Storage (SAN/NAS) Encryption – provides for encrypting large volumes of active data/information. Mass storage devices refer to storage area networks (SAN) and network-attached storage (NAS) data management solutions. Recently, the boundaries between NAS and SAN systems have overlapped with some products providing both file level protocols (NAS) and block level protocols (SAN).

Mass Storage (SAN/NAS) Encryption should have the following capabilities: Supports encryption throughout the lifecycle of all data/information whether in storage or in transit; encryption and decryption methods must have both logical and physical segmentations; provide efficient encryption/decryption across multiple mass storage device types including fiber channel disks within an IP based network environment.

[8] S720 Platform Infrastructure Standard; S730 Application and Related Software Standards; S731 Software Productivity Tools Standard; Target Platform Table at http://www.azgita.gov/enterprise_architecture/NEW/Platform_Arch/platform_assess.htm ; Target Software Table at http://www.azgita.gov/enterprise_architecture/NEW/Software_Arch/appendix%20C.pdf ; and Target Technology OSI Table at http://www.azgita.gov/enterprise_architecture/AZ_EA_Target_Technology_Table.htm .

4.2.5 Database Encryption – entails encrypting physical data within a database by encrypting the entire database, or calling functions, or stored procedures and database triggers, or natively using Database Management Systems (DBMS) encryption features to encrypt all or in part (column, row, or field level). Database encryption can be implemented at the application level.

Database Encryption should have the following capabilities: Supports symmetric and asymmetrical encryption; ability to perform column/row level encryption vs. full database encryption for greater flexibility; supports multiple database platforms and operating systems; ability to encrypt and decrypt at the application and/or field level; supports separation of duties for Database Administrator's (DBA's) and the "KEY" Administrator.

4.2.6 Encryption for Removable Storage Drives and Devices – provides encryption for smaller portable devices and existing data-sets. A USB flash drive comprises a memory card that plugs into a computer's USB port and functions as a portable hard-drive that does not contain moving parts. USB flash-drives are also known as a "flash drive," "thumb drive," "pen drive," "keychain drive," "key drive," "USB key," "USB stick" and "memory key."

Encryption for Removable Storage Drives and Devices should have the following capabilities: USB flash-drives must have password/security capabilities built into the device. USB flash-drives and removable storage devices can be bought with encryption software installed on the device hardware, or file-encryption software can be purchased after-the-fact for installation.

4.3 Wireless Encryption Technologies

All public and confidential information transmitted through wireless technologies shall be deployed through the IEEE 802.11 standard for WLANs (Wireless Local Area Networks). The Wireless Protected Access2 (WPA2) protocol with AES encryption shall be deployed for data encryption to further protect transported information from intruders and eavesdroppers. Current versions of IEEE standards are 802.11, 802.11a, 802.11b, 802.11e, 802.11g, 802.11i and 802.11n.

4.3.1 All Budget Units shall deploy 802.11g or greater for WLAN and WMAN[9] wireless communications and encryption. 802.11g can update drivers to support WPA2.

4.3.2 Wireless technologies generally come with some embedded security features of which many are disabled by default and all Budget Units shall review and enable such features as appropriate. While some security features have some vulnerabilities and weakness, they still

[9] Wireless Metropolitan Area Networks (WMAN) provide connectivity to users located in multiple facilities that are generally within a few miles of each other and allows for large data transmissions with minimal interference.

provide a substantial degree of protection against unauthorized disclosure, access, and other active-probing attacks.

4.3.3 Budge Units shall also deploy higher-level encryption protocols and applications, such as secure shell (SSH), Transport-Level Security (TLS) and the Internet Protocol Security (IPsec) associated algorithms to protect transported information, regardless of whether nonvalidated data-link security-protocols are used.

4.3.4 Budget Units shall routinely test inherent security features of both 802.11g or greater and WPA2 as an overall defense-in-depth strategy to attain the highest levels of integrity, authentication, and confidentiality. Budget Units shall also carefully consider deployment of robust and proven security features as listed below:

a. Authentication and encryption algorithms;

b. Bluetooth and built-in security features (data-link-level encryption and authentication protocols)[10];

c. Firewalls and other appropriate protection and intrusion mechanisms.

4.3.5 Wireless configurations managed by Budget Units shall comply with all aspects of wireless security and architecture as defined in *Statewide Standard P800-S830 Network Security*, section 4.6 "External Connections to Networks", section 4.8 "Wireless Network Access" and *Statewide Standard P700-S710 Network Infrastructure*, section 4.4, "Wireless Network Connectivity".

4.4 <u>Encryption Architecture and Best Practices</u> -Encryption Technologies shall:

4.4.1 Be processed and stored as a C2 Level of Trust when data/information is encrypted and transmitted through Budget Unit networks. This level of security is applied to operating-systems software of all client devices configured on a network. C2 is an industry-rating for business computing products and requires that all network systems have discretionary resource-protection and auditing capability.

4.4.2 Be managed and controlled by Budget Units in addition to encryption keys (Key Management) used in any encrypted transmissions except as noted in section 4.1.9 of this document.

4.4.3 Have sufficient capacity and redundancy incorporated into the Budget Units network system to further prevent the transmission of confidential information in clear text;

4.4.4 Support all state operating systems and platforms[11] as identified in *Statewide Standard P700-S720 Platform Infrastructure*;

---

[10] See S830 Network Security Standard for security services and security modes 1, 2, and 3 for Bluetooth.

[11] The term "platform" applies to servers, storage, and end-user (client) devices, including portable devices, with respective operating systems, interfaces, and drivers that provide a framework for interoperability, scalability, and portability. S720 Platform Infrastructure Standard; S730 Application and Related Software Standards; S731 Software Productivity Tools Standard; Target Platform Table at http://www.azgita.gov/enterprise_architecture/NEW/Platform_Arch/platform_assess.htm ;

4.4.5 Support current communication and security protocol standards as identified in the *Statewide Standards P700-S710 Network Infrastructure and P800-S830 Network Security*;

4.4.6 Be non-proprietary and supports compression capabilities;

4.4.7 Take advantage of 32 and 64-bit architecture;

4.4.8 Supports 256 encryption key lengths. Budget Units with deployed 128 encryption key lengths are grand-fathered for a period of three years from an effective date of April 2, 2008;

4.4.9 Provide auditing, alert notification, logging and performance monitoring capabilities;

4.4.10 Provide access control to view audit data and encrypted audit data as well as logs; shall also be interoperable with computer forensic software;

4.4.11 Provide authentication options that includes one or more of the following: Microsoft Graphical Identification and Authentication (GINA) for single sign-on; User ID/Password; Smart Cards; Token (USB), Biometrics; Trusted Platform Module (TPM) and Kerberos;

4.4.12 Support integration with Lightweight Directory Active Protocol (LDAP) utilizing common implementation strategies (e.g., MS Active Directory, Novell, eDirectory, etc.)

4.4.13 Support disk sanitization procedures in accordance with the National Institute of Standards and Technology (NIST) specifications;

4.4.14 Support multiple partitions on a disk or disk volume and disk re-imaging;

4.4.15 Have the ability to securely delete data/information, including temporary files;

4.4.16 Shall provide transparent encryption/decryption of data and files to the user once the disks are fully encrypted or the client is fully configured;

4.4.17 Provide remote password reset for offline end-users needing assistance;

4.4.18 Support single sign-on methods where users can authenticate with Active Directory credentials and password synchronization with no user interaction;

4.4.19 Be compatible with major anti-virus mal-ware products to include at a minimum: Symantec, McAfee, CA, and Microsoft;

4.4.20 Support Digital Rights Management (DRM) capabilities;

4.4.21 Support scalability in terms of configuration options with fixed devices, mobile devices, email security, file sharing, etc;

4.4.22 Provide version insurance and support for three years and provide one-year notification for any product version retirements;

4.4.23 Provide effective central management controls for management of end users/customers;

4.4.24 Be easily configured and/or customized for different locations and/or end-users, both locally and remotely;

4.4.25 Provide an alert notification function/capability in the event of an attack (unauthorized access attempt) on a device.

4.5 NOTICE OF INTENT (NOI) ENCRYPTION READINESS CHECKLIST:

4.5.1 All Budget Units shall submit a Notice of Intent (NOI) before starting an encryption implementation project. The NOI will be used by GITA to review and analyze general project information, encryption methods and solutions, estimated costs and signature approvals.

4.5.2 A template for the NOI Encryption document shall be maintained by GITA and available to Budget Units by accessing the following web site: http://www.azgita.gov/sispo/NOI/.

4.5.3 A high level overview of the NOI Encryption review process is also listed at the following web site: http://www.azgita.gov/sispo/NOI/.

4.6 NOI Encryption Evaluation – GITA shall evaluate submitted NOI's based on the following criteria[12]:

4.6.1 Project scope, including a description of costs, technical solution proposed, hosting, and a plan for ongoing maintenance.

4.6.2 Completeness of content, including contact information, detailed project description, and business need.

4.6.3 Presence of sufficient information to determine that the project does not replicate and or overlap existing encryption efforts by other state divisions and/organizations.

4.6.4 Presence of authorization signatures.

4.6.5 Upon completion of GITA's review and evaluation, a letter of response may be issued to the budget unit requesting further information about the proposed encryption project.

4.6.6 If the NOI is considered incomplete, GITA shall return the NOI to the submitting Budget Unit identifying such incomplete items.

a. The Budget Unit may resubmit a revised document at its convenience.

b. The Budget Unit may withdraw an NOI from review at any time.

[12] Executive Order 2008-10 Item 4.

4.6.7 When total costs for an NOI exceed $25,000, the Budget Unit shall obtain project approval through the Project Investment Justification (PIJ) rather than the NOI. This is in compliance with the *Statewide Policy P340, PIJ and Statewide Standard P340-S340, PIJ.*

a. When a PIJ is required, the project summary report, described in Statewide Procedure S340-P340, PIJ shall replace the written review on the conformance of encryption technologies to published standards. For additional information refer to http://www.azgita.gov/project_investment_justification/.

4.7 NOI Encryption Approval

4.7.1 GITA shall prepare and submit a written review to the State CIO and state whether the NOI project meets all the above criteria in this standard and recommendations for approval, conditional-approval or not-approved.

4.7.2 The State CIO shall transmit a letter of response to the Budget Unit Director and CIO that describes the results of the NOI review. The letter of response shall contain recommendations for approval, or conditional approval, or not-approved.

5. DEFFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the GITA website at 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 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 Statewide Policy P100, Information Technology.
6.16 Statewide Policy P800, IT Security.

6.17 State of Arizona Target Security Architecture, http://www.azgita.gov/enterprise_architecture.
6.18 A.R.S. § 41-132 Electronic and Digital Signatures
6.19 Arizona Administrative Code Title 2, Administration, Chapter 12, Office of the Secretary of State, Article 5, Electronic Signatures.
6.20 Secretary of State Electronic Signature Policies and Procedures (http://www.azsos.gov/pa)
   A. Policy Authority Procedures – Introduction
   B. Policy Authority Procedures for AESI – Overview
   C. Policy Authority Procedures – Forward
   D. Policy Authority Procedures; Section 3.6 – Identification and Authentication
   E. PKI Certificate Policy (in "Certificate Policy")
   F. PGP Certificate Policy
   G. Considerations for Agencies Contemplating Electronic Signature Pilot Projects
   H. Arizona Electronic Signature Infrastructure (AESI) – Definitions and Acronyms
   I. Arizona Electronic Signature Infrastructure (AESI) – Miscellaneous Exhibits

7. ATTACHMENTS

None.