Terry Goddard
Attorney General

Office of the Attorney General
State of Arizona

Arizona Attorney General's Office
(602) 542-9173

Attorney General Certification Statement

The Arizona Attorney General's Office has reviewed the Arizona Department of Environmental Quality's application and supporting documentation to EPA to approve electronic reporting.

This Office certifies:

1. that the State of Arizona has sufficient legal authority provided by Arizona's lawfully enacted or promulgated statutes or regulations to implement the electronic reporting component of its authorized programs consistent with 40 Code of Federal Regulations § 3.2000 and with this application;

2. that such statutes or regulations are in full force and effect on the date of this certification; and

3. that Arizona has authority to enforce the affected programs using electronic documents collected under these programs.

We have included with this certification all Arizona statutes and regulations relevant to this application. To assist EPA's review of this application, We also have included a description specifically linking applicable provisions of 40 C.F.R. Part 3 with relevant portions of Arizona's statutes and regulations.

Terry Goddard January 14 2010

Terry Goddard — date
Arizona Attorney General

STATEMENT IN SUPPORT OF THE ARIZONA DEPARTMENT OF ENVIRONMENTAL QUALITY'S APPLICATION FOR ELECTRONIC REPORTING

Certification of Legal Authority for Electronic Reporting as Required by Cross Media Electronic Reporting Regulations (CROMERR), 40 CFR Part 3

In accordance with Arizona statutes and rules described herein, Arizona has sufficient authority to implement electronic reporting consistent with 40 CFR Part 3.

Sources of Authority

Federal Authority:

40 CFR Part 3, §3.1000(b)(1)(i)

40 CFR Part 3, §3.2000(b)

State Authority

A.R.S. Title 44, Chapter 2. Arizona Electronic Transactions Act

A.R.S. § 41-132 Electronic Signatures

A.A.C. R2-12-501 Electronic Signatures

A.R.S. § 13-2001, *et seq*. Forgery and Other Offenses

A.R.S. § 13-2300 *et seq*. Organized Crime and Fraud

http://www.azgita.gov/nav/e_gov.htm Arizona Government Information Technology Agency (E-Government Services)

http://www.azgita.gov/policies_standards/ Arizona Government Information Technology Agency Policy and Standards index page.

http://www.azgita.gov/policies_standards/pdf/p800%20securtiy%20policy.pdf GITA standards Statewide Policy P800 Rev 3.0.

(http://www.azgita.gov/policies_standards/pdf/p800-s820%20authentication%20standard.pdf) GITA Statewide Policy P800-P820 Rev. 2.0 Authentication and Directory Services

Arizona has the legal authority to implement electronic reporting

CROMERR requires that the State of Arizona must have "sufficient legal authority provided by lawfully enacted or promulgated statutes or regulations that are in full force and effect on the date of the certification to implement the electronic reporting ...." 40 CFR 3.1000(b)(1)(i). The electronic reporting must conform to the requirements of 40 CFR 3.2000. Id.

The Arizona Electronic Transactions Act A.R.S. § 44-7001 *et seq.* provides for the use of electronic signatures when a person transacts business with the State. In particular, "A record or signature in electronic form cannot be denied legal effect and enforceability solely because the record or signature is in electronic form." A.R.S. § 44-7007(A). Additionally, A.R.S. § 44-7007(C) provides that "an electronic record satisfies any law that requires a record be in writing." Also, "An electronic signature satisfies any law that requires a signature." A.R.S. § 44-7007(D). Finally, no electronic documents or signatures may be excluded from evidence solely because they are in electronic form. A.R.S. § 44-7013.

Electronic signatures have the "same force and effect as a written signature" provided certain requirements are met. A.R.S. § 41-132(A). Those requirements are enumerated in A.R.S. §§ 41-132(B, C).

Arizona Government Information Technology Agency

Government Information Technology Agency (GITA) is an Arizona State agency established pursuant to A.R.S. § 41-3501 *et seq.* which is responsible for adopting, *inter alia*, statewide "security standards for information technology." A.R.S. § 41-3504(A)(1)(a). A.R.S. § 44-7041 *et seq.* sets forth the requirements for electronic government records and how they must conform to GITA requirements. Additionally, A.A.C. R2-12-504(A) requires: "The Secretary of State shall accept, and approve for use, technologies for electronic signature, in consultation with the Policy Authority and GITA, provided the technologies meet the standards set forth in the GITA standards for Electronic Signatures, as specified in A.R.S. § 41-3504."

GITA has reviewed the ADEQ programs and determined that they are fully complaint with the requirements of GITA. The policies governing the use of secure electronic transactions are available at: http://www.azgita.gov/policies_standards/

Under the GITA standards Statewide Policy P800 Rev 3.0 (GITA Policy P800 Rev. 3.0) (http://www.azgita.gov/policies_standards/pdf/p800%20securtiy%20policy.pdf), the IT security responsibilities are outlined in Sec. 4.1. In particular, the program will "guard against improper information modification or destruction, and include ensuring information non-repudiation and authenticity ...." Sec. 4.1.1. Section 4.1.3 also requires that "data/information contained in electronic transactions is protected via: 1) identification, authentication, and authorization; 2) encryption; and, 3) electronic signature, as necessary."

Additionally, Statewide Policy P800-P820 Rev. 2.0 Authentication and Directory Services (GITA Policy P800-S820 Rev. 2.0) (http://www.azgita.gov/policies_standards/pdf/p800-s820%20authentication%20standard.pdf) details the standard for authentication of information submitted to the State. ADEQ uses the Authentication by Knowledge standard outlined in Section 4.1. Authentication by Knowledge is a system whereby the identity of the person submitting the information is verified by that person's knowledge of certain information that is only know to that person, such as user name and password.

CROMERR and Arizona Law

Under 40 CFR 3.2000(a), "Authorized programs that receive electronic documents in lieu of paper must: 1) use an acceptable electronic document receiving system as specified under paragraphs (b) and (c) of this section." Additionally, the program must "require that any electronic document must bear the valid electronic signature of a signatory ...." The Code continues with details of the technical requirements that electronic signatures must comply with to be eligible for certification under CROMERR. The following is a detailed analysis of the CROMERR requirements and applicable Arizona standards:

40 CFR 3.2000(b)

This section requires that electronic documents be able to generate data sufficient to ensure that the document is, *inter alia*, true, accurate, complete, unaltered and was submitted knowingly. In addition, GITA Policy P800, Rev. 3.0 Section 4.1 enumerates the standards that coincide with the CROMERR requirements. In particular, Section 4.1.3 requires that the system "Ensure that data/information contained in electronic transactions is protected via 1) identification, authentication, and authorization; 2) encryption; and, 3) electronic signature, as necessary." This requirement is satisfied under Arizona law in A.R.S. §§ 41-132(A), 44-7007(A, C, and D) because electronic documents are legally the equivalent of written documents. Moreover, such electronic documents are admissible under A.R.S. § 44-7013.

40 CFR 3.2000(b)(1)

This section requires the electronic document be able to show that "the electronic document was not altered without detection during transmission or at any time after receipt." This provision is satisfied by GITA Policy P800, Rev. 3.0 Section 4.1.1 (requiring the system provide: "integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity[.]" *See also;* A.R.S. § 41-132(C)(3) which requires that digital signatures be capable of verifying not only that the document was created using the digital key, but that the document was not altered.

40 CFR 3.2000(b)(2)

This section requires that "any alteration to the electronic document during transmission or after receipt are fully documented." This provision is met under §4.1.1 ("[G]uard against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.") and §4.1.3 ("Provide adequate security for all information collected, processed, transmitted, stored, or disseminated …") of GITA Policy P800 Rev. 3.0.

40 CFR 3.2000(b)(3)

This section requires that "The electronic document was submitted knowingly and not by accident." Section 4.1.1 of GITA Policy P800 Rev. 3.0 requires "that actions of individuals or entities can be traced to the individual or entity, non-repudiation ...." Non-repudiation is where the submitter cannot repudiate either the contents of the submission or its submission. Also, under §4 of GITA Policy P800-S820 Rev. 2.0, only a user who knows certain specific information, such as user name and password, may even access the system.

40 CFR 3.2000(b)(4)

This section requires: "Any individual identified in the electronic document submission as a submitter or signatory had the opportunity to review the copy of record in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or labeling of the information and had the opportunity to repudiate the electronic document based on this review." Section 4.1.1 of GITA Policy P800 Rev. 3.0 requires "actions of individuals or entities can be traced to the individual or entity, non-repudiation, and security review controls and procedures ...." Also, under §4 of GITA Policy P800-S820 Rev. 2.0, only a user who knows certain specific information, such as user name and password, may even access the system..

40 CFR 3.2000(b)(5)

This section has several requirements, each of which will be dealt with in turn.

i) "The electronic signature was valid at the time of signing." This requirement is met under §§4.1.1 and 4.1.3 GITA Policy P800-S820 Rev. 2.0 (which require authentication by the person submitting the data and that it is protected by "identification, authentication, and authorization ..." by the person submitting it) and §4 of GITA Policy P800-S820 Rev. 2.0 (only a user who knows certain specific information, such as user name and password, may even access the system).

ii) "The electronic document cannot be altered without detection at any time after being signed." This requirement is met under §4.1.1 of GITA Policy P800

Rev. 3.0, §4 of GITA Policy P800-S820 Rev. 2.0, and A.R.S. § 41-132(C)(3)(b).

iii) The signatory had the opportunity to review the content prior to signing. This requirement is met under §4.1.1 of GITA Policy P800 Rev. 3.0 and §4 of GITA Policy P800-S820 Rev. 2.0.

iv) The signatory had the opportunity to review the content or meaning of the certification statement including that false certification contains criminal penalties. This requirement is met under §4.1.1 GITA Policy P800 Rev. 3.0 and §4 of GITA Policy P800-S820 Rev. 2.0.

v) The signatory has signed an electronic signature or subscriber agreement. This requirement is met under §§4.1.1, 4.1.3 of GITA Policy P800 Rev. 3.0 and §4 of GITA Policy P800-S820 Rev. 2.0.

vi) The receiving system has automatically responded to the receipt of the electronic document with an acknowledgment that identifies the electronic document received, the signatory, time, date and is sent to at least one address that does not share the same access controls as the account used to make the electronic submissions. In this case, the receiving system is the GITA portal (www.AZ.gov). The GITA portal is fully complaint with §4.1.3 GITA Policy P800 Rev. 3.0 and §4 of GITA Policy P800-S820 Rev. 2.0, Authentication by Knowledge.

vii) "For each electronic signature device used to create an electronic signature, the identity of the individual uniquely entitled to use the device and his relation to the entity for which the documents are submitted is determined to a legal certainty ...." This requirement is met under §4.1.1 of GITA Policy P800 Rev. 3.0 and §4 of GITA Policy P800-S820 Rev. 2.0.

40 CFR 3.2000(c)

This section requires that: "A person is subject to any appropriate civil penalties, criminal penalties or remedies ... for failure to comply with a reporting requirement if the person fails to comply with the applicable provision for electronic reporting." 40 CFR 3.2000(c)(1). Additionally, the electronic document must "legally bind or obligate the

signatory ... to the same extent as the signatory's handwritten signature ..." 40 CFR 3.2000(c)(2). The electronic signature must also establish that the individual uniquely qualifies to use the device did so with the intent to sign ...." 40 CFR 3.2000(c)(3). Finally, the electronic document must be freely admissible in evidence in enforcement proceedings. 40 CFR 3.2000(c)(4).

If a person attempts to submit electronic reports to ADEQ, the submission process protocols embodied at the state portal prevent improper submissions. The individual environmental programs that ADEQ administers all have provisions based in federal law and state law that provide for various civil and criminal penalties for failure to comply with reporting requirements. These include, *inter alia*, the Clean Water Act (A.R.S. § 49-255 *et seq*. 33 U.S.C.A. § 1251 *et seq*.), Clean Air Act (A.R.S. § 49-401 *et seq*. 42 U.S.C.A. § 7401 *et seq*.), Resource Conservation and Recovery Act (A.R.S. § 49-901 *et seq*., 42 U.S.C.A. § 6901 *et seq*.), and the Underground Storage Tank Act (A.R.S. § 49-1001 *et seq*., 42 U.S.C.A. § 6991 *et seq*.). Under the Arizona Electronic Transaction Act, A.R.S. Title 44, Chapter 2, electronic documents have the same force and effect as written documents. Finally, as discussed, *supra,* the GITA policies and portal are designed to ensure that the electronic documents are traced to specific persons and that submission of that document is non-repudiable and the process is secure.

Arizona Criminal Enforcement

The Arizona Criminal Statutes provide sufficient authority to enforce electronic reporting to meet the requirements of CROMERR.[1] This conclusion is based on the following statutes.

Criminal enforcement provisions are based upon the scheme of misdemeanor and felony classifications and punishments set forth in the Arizona Criminal Code, A.R.S. § Title 13, and include imprisonment and fines. Sentencing for felonies in Arizona is controlled by A.R.S. § 13-702. Generally, the felony scheme starts with a Class 6 felony (the least

[1] The term "written instrument" does include "or equivalent" which under A.R.S. § 44-7001 *et seq*., includes an electronically generated document. A.R.S. § 13-2001(11).

serious) and progresses to a Class 1 felony (the most serious). A first-time offender is subject to a presumptive term of imprisonment subject to a finding of certain aggravating or mitigating factors. A court may increase or decrease sentences based on aggravating and mitigating factors listed in A.R.S. § 13-701(D, E). An increase or decrease in sentence must fall within the ranges specified in A.R.S. § 13-702(D). Under A.R.S. § 13-708, multiple sentences are served consecutively. The terms of imprisonment for repeat offenders increase with the number of prior felony convictions as delineated in A.R.S. § 13-604.

Under A.R.S. § Title 13, the maximum criminal fine applicable to an individual convicted of a felony is $150,000. A.R.S. § 13-801. The maximum criminal fine applicable to an enterprise is one million dollars. A.R.S. § 13-803. An enterprise includes "any corporation, association, labor union or other legal entity." A.R.S. § 13-105(15). Moreover, a fine for an enterprise my be increased five-fold if certain aggravating factors are present. A.R.S. § 13-823. Finally, all criminal and civil penalties are increased by 77% due to several statutory surcharges. See: A.R.S. § 12-116.01(A)(adding a 47% surcharge), A.R.S. § 12-116.01(B) adding a 7% surcharge), A.R.S. § 12-116.02(A)(adding a 13% surcharge), and A.R.S. § 16-954(C)(adding a 10% surcharge).

A.R.S. § 13-2002 (Forgery):

"A person commits forgery if, with intent to defraud, the person: (1)falsely makes, completes or alters a written instrument …." Forgery is a class 4 felony. A "written instrument" means either; (a) any paper, document or other instrument that contains written or printed matter or its equivalent. …" Equivalent documents include electronic documents. A.R.S. § 44-7007(C).

A.R.S. § 13-2310(A) Fraudulent Schemes and Artifices

Any person who, pursuant to a scheme or artifice to defraud, knowingly obtains any benefit by means of a false or fraudulent pretenses, representations, promises or material omissions is guilty of a class 2 felony. Attempting to obtain the benefit of complying

with ADEQ reporting requirements through the submission of a false electronic document may be a fraudulent scheme and artifice under Arizona criminal law.

A.R.S. § 13-2311(A) Fraudulent Schemes and Practices

"[I]n any matter related to the business conducted by any department or agency of this state or any political subdivision thereof, any person who, pursuant to a scheme or artifice to defraud or deceive, knowingly falsifies, conceals or covers up a material fact by any trick, scheme or device or makes or uses any false, fictitious or fraudulent statement or entry is guilty of a class 5 felony." Attempting to obtain the benefit of complying with ADEQ reporting requirements through the submission of a false electronic document may be a fraudulent scheme and practice under Arizona criminal law.

A.R.S. § 13-2008(A) Taking the identity of another person

(A) A person commits taking the identity of another person if the person takes or uses any personal identifying information[2] of another person, without the consent of that person, with the intent to obtain or use the other person's identity for any unlawful purpose or to cause loss to a person. This is a class 4 felony. A person who submits an electronic document using the login name and password of another may be guilty of taking the identity of another under Arizona criminal law.

40 CFR 3.2000(c)(2)

This section requires that an electronic document "submitted to satisfy a state ... reporting requirement bears an electronic signature, the electronic signature legally binds or obligates the signatory, or makes the signatory responsible, the same extent as the

---

[2] A.R.S. Title 13. A.R.S. § 13-2001(10) defines "personal identifying information" to mean "any written document or electronic data that does or purports to provide information concerning a name, signature, electronic identifier or screen name, electronic mail signature, address or account, biometric identifier, driver or professional license number, access device, residence or mailing address, telephone number, employer, student or military identification number, social security number, tax identification number, employment information, citizenship status or alien identification number, personal identification number, photograph, birth date, savings, checking or other financial account number, credit card, charge card or debit card number, mother's maiden name, fingerprint or retinal image, the image of an iris or deoxyribonucleic acid or genetic information."

signatory's handwritten signature on a paper document ..." This requirement is met under §4 of GITA Policy P800-S820 Rev. 2.0. *See* also: A.R.S. § 41-132(A).

40 CFR 3.2000(c)(3)

This section requires that a particular electronic signature device was used to "create an electronic signature that is included in or logically associated with an electronic document ... will suffice to establish that the individual uniquely entitled to use the derived at the time of signature did so with the intent to sign the electronic document and give it effect." This requirement is met under §4 of GITA Policy P800-S820 Rev. 2.0. *See also*: A.R.S. § 41-132(B) and A.R.S. § 41-132(E)(4). This requirement is also met under §4 of GITA Policy P800-S820 Rev. 2.0.

40 CFR 3/2000(c)(4)

This section requires that "[n]othing in the authorized program limits the use of electronic documents or information derived from electronic documents as evidence in enforcement proceedings." *See:* A.R.S. § 41-132(A), A.R.S. § 41-132(E)(4), A.R.S. § 44-7013.

462234.2

STATE of ARIZONA

Government Information Technology Agency	**Statewide POLICY**	**TITLE: IT Security**
	P800 Rev 3.0	**Effective Date: December 12, 2008**

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 adopting statewide technical, coordination, and IT policy and standards (A.R.S. § 41-3504(A (1(a)))).

2. **PURPOSE**
To establish a statewide security policy for the protection of IT assets and resources, including data/information for Budget Units with their own network infrastructure and for those that have implemented the AZNET program for network services.

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. **POLICY**
The State of Arizona shall securely and economically protect its business functions, including public access to appropriate information and resources, while maintaining compliance with the legal requirements established by existing Federal and State statutes pertaining to confidentiality, privacy, accessibility, availability, and integrity.

Budget Units that are maintaining their own network infrastructure shall tightly integrate its security architecture/technologies with common services including Remote Access, Internet Access, Firewall, VPN, Spam and Anti-Virus Email Filtering, and other services that comply with this policy and related IT security standards in addition to the AZNET program.

Budget Unit's that have implemented the AZNET program for network services, security architecture/technologies are specifically designed to support and

integrate tightly with a converged network that offers security for common services including Remote Access, Internet Access, Firewall, VPN, Spam, and Anti-Virus Email Filtering, and other services that comply with this policy and related IT security standards. AZNET's security program will further eliminate unauthorized third party Internet connections in addition to improving the State's network security posture through a centralized security infrastructure.

4.1. IT SECURITY POLICY RESPONSIBILITIES

The policy establishes that budget units shall:

4.1.1. Protect the State's IT assets, resources, and data/information from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
- Confidentiality, which means preserving authorized restrictions from access and disclosure, including means for protecting personal privacy and proprietary information;
- Availability, which means ensuring timely and reliable access to and use of information. Availability is securely accomplished through identification, authentication, authorization and access control;
- Accountability, which includes requirements that actions of individuals or entities can be traced to the individual or entity, non-repudiation, and security review controls and procedures; and
- Assurance, including security administration and adherence to Statewide IT security policies and standards.

4.1.2. Provide security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, modification to, or destruction of either 1) information collected or maintained by or on behalf of the budget unit or 2) information systems used by a budget unit or by a contractor of a budget unit or other organization on behalf of the budget unit.

4.1.3. Ensure that data/information contained in electronic transactions is protected via 1) identification, authentication, and authorization; 2) encryption; and 3) electronic signature, as necessary.

4.1.4. Provide adequate security for all information collected, processed, transmitted, stored, or disseminated in budget unit software application systems.

4.1.5. Ensure that networks, hardware systems, and software application systems operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

4.1.6. Apply security controls to information systems, resources, and data/information sufficient to contain risk of loss or misuse of the information to an acceptable level that supports the mission and operation of the budget unit.

4.1.7. Ensure that information security management processes are integrated with budget unit strategic and operational planning processes, including planning and implementing (see paragraph 4.6) any necessary remedial action to address IT security deficiencies.

4.1.8. Communicate applicable Statewide and budget-unit-specific IT security policies and standards to appropriate third-party organizations.

4.1.9. Establish IT security programs, including assignment of roles and responsibilities, as well as creation of any necessary procedures, adherence requirements, and monitoring controls that adhere to:

- *Statewide Policy P800, IT Security*;
- Applicable Statewide Standards for IT security; and
- Budget-unit-specific IT security policies, standards, and procedures.

Budget unit IT security programs shall be appropriate to each budget unit's operational and technology environment in order to provide a foundation for management to make informed decisions and IT investments that appropriately mitigate IT security risks to an acceptable level.

4.1.10. Identify, define, and resolve overlapping IT security roles/responsibilities between budget units and/or contractors relative to security services received from, or provided to, other budget units. Security services received from, or provided to, other budget units should be defined by an Inter-agency Service Agreement (ISA).

4.2. SECURITY ARCHITECTURE PRINCIPLES

The planning, design, and development of Security Architecture are guided by the following general principles that support the State's strategic business goals and objectives.

4.2.1. Security Architecture shall enable the State and its budget units to perform business processes electronically and deliver secure e-government services to the public.

4.2.2. Security levels applied to systems and resources shall, at a minimum, be commensurate with their value to the State and its budget units, and sufficient to contain risk to an acceptable level.

4.2.3. Security Architecture shall be based on industry-wide, open standards, where possible, and accommodate varying needs for and levels of security.

4.2.4. Security is a critical component of individual budget unit and State systems interoperability.
4.2.5. Security architecture shall accommodate varying security needs.

Supporting rationale for the above principles can be found in the *State of Arizona Target Security Architecture* document available at http://www.azgita.gov/enterprise_architecture.

4.3. SECURITY ARCHITECTURE TARGET TECHNOLOGIES
Components of the Target Security Architecture are reviewed and refreshed on a regular and scheduled basis to address major shifts in technology, as well as the emergence and adoption of new technology-related industry or open standards. Review criteria shall adhere to the lifecycle process described in *Statewide Policy P700, Enterprise Architecture*.

4.4. SECURITY ARCHITECTURE STANDARDS
Security Architecture defines common, industry-wide, open-standards-based technologies required to enable secure and efficient transaction of business, delivery of services, and communications among its citizens, the federal government, cities, counties, and local governments, as well as the private business sector. Security Architecture Standards allow the State and individual budget units to quickly respond to changes in technology, business, and information requirements without compromising the security, integrity, and performance of the enterprise and its information resources. Refer to Paragraph 6.20, Statewide Standards for Security Architecture, for further information.

4.5. IMPLEMENTATION
Arizona's EWTA has been designed to maximize current investments in technology, provide a workable transition path to targeted technologies, maintain flexibility, and to enhance interoperability and sharing. Security Architecture implementations shall adhere to implementation strategies described in *Statewide Policy P700, Enterprise Architecture*. Security Architecture shall be implemented in accordance with this policy, applicable statewide standards for security, and relevant Federal, and individual budget unit standards.

4.6. CONFORMANCE OF IT INVESTMENTS AND PROJECTS TO EA
To achieve the benefits of an enterprise-standards-based architecture, all information technology investments shall conform to the established EWTA that is designed to ensure the integrity and interoperability of information technologies for budget units. *Statewide Standard P340-S340, Project Investment Justification (PIJ),* defines conformance with the established EWTA and associated Statewide Policies and Standards. Variances from the established EWTA shall be documented and justified in the appropriate section of the PIJ document.

4.7. APPLICABILITY TO OTHER STATEWIDE EA POLICIES AND STANDARDS

Statewide Policy P800, IT Security, adheres to and demonstrates the purpose established in *Statewide Policy P100, Information Technology*. *Statewide Policy P800, IT Security*, adheres to the principles, governance, lifecycle process, and implementation elements described in *Statewide Policy P700, Enterprise Architecture*.

5. DEFINITIONS 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. Federal Office of Management and Budget (OMB) Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources."
6.16. State of Arizona Target Security Architecture.
6.17. Statewide Policy P100, Information Technology.
6.18. Statewide Policy P340, Project Investment Justification (PIJ).
  6.18.1. Statewide Standard P340-S340, Project Investment Justification.
6.19. Statewide Policy P700, Enterprise Architecture.
6.20. Statewide Policy P800, IT Security.
  6.20.1. Statewide Standard P800-S805, IT Risk Management.
  6.20.2. Statewide Standard P800-S810, Account Management.
  6.20.3. Statewide Standard P800-S815, Configuration Management.
  6.20.4. Statewide Standard P800-S820, Authentication and Directory Services.

6.20.5. Statewide Standard P800-S825, Session Controls.
6.20.6. Statewide Standard P800-S830, Network Infrastructure.
6.20.7. Statewide Standard P800-S850, Encryption Technologies.
6.20.8. Statewide Standard P800-S855, Incident Response and Reporting.
6.20.9. Statewide Standard P800-S860, Virus and Malicious Code Protection.
6.20.10. Statewide Standard P800-S865, IT Disaster Recovery Planning (DRP).
6.20.11. Statewide Standard P800-S870, Backups.
6.20.12. Statewide Standard P800-S875, Maintenance.
6.20.13. Statewide Standard P800-S880, Media Sanitizing/Disposal.
6.20.14. Statewide Standard P800-S885, IT Physical Security.
6.20.15. Statewide Standard P800-S890, Personnel Security.
6.20.16. Statewide Standard P800-S895, Security Training and Awareness.

7. ATTACHMENTS

None.

STATE of ARIZONA

Government Information Technology Agency	**Statewide STANDARD**	**TITLE: Authentication and Directory Services**
	P800-S820 Rev 2.0	**Effective Date: September 12, 2008**

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 provide identification and authentication methods for information systems used by customers/users that access resources or services through state application systems. Identification, authentication and directory services provide the foundation for securing data/information for 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 organization receiving, expending or disbursing state funds or incurring obligations of the state including the Arizona Board of Regents 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

Identification, authentication and directory services are a crucial security step for proper access and authorization to application systems that provide non-repudiation, and auditing capabilities for budget units. Without authentication, budget units have no assurance that access to resources and services are properly managed, controlled, and monitored.

To safeguard critical application systems, information, and networks from unauthorized access or intrusions, budget units shall ensure identity and authentication of a user/customer before granting access to resources and services by implementing one or more of the following authentication methods:

- ***Authentication by Knowledge*** – Based on information only the user knows;
- ***Authentication by Ownership*** – Based on something only the user possesses;
- ***Authentication by Characteristic*** – Based on a user's physical characteristic.

4.1. AUTHENTICATION BY KNOWLEDGE - User authentication shall be based on the presence of a userID associated with something only the user/customer knows and shall include the following:

4.1.1. Password – A secret series of characters that, by association with a userID, enables a user to access information, systems, applications, or networks. Budget units shall establish, implement, document, and communicate (in accordance with Statewide Standard P800-S895, Security Training and Awareness) criteria governing the following:

- A consistent treatment used throughout the budget unit (a mixture of upper/lower case characters, numbers, and special characters is recommended),
- Minimum password length and format,
- Maximum validity periods for passwords (passwords should be automatically set to expire),
- Password reuse limitations,
- Number of unsuccessful login attempts allowed, and
- Procedures for revoking and resetting passwords.

Use of passwords shall conform to the following requirements:

- Passwords shall be for individual users in order to maintain accountability. Generic, multi-user IDs should be eliminated
- Passwords shall be different from userIDs.
- Passwords shall be kept confidential.
- Passwords shall not be displayed when entered.
- Passwords shall not be transmitted in clear text format.
- Passwords shall not be kept on paper or stored in plain text format.
- Passwords shall be changed whenever there is a chance that the password or the system has been compromised.
- Passwords shall be changed periodically and not reused.
- Passwords shall not be included in a macro or function key to automate log-in processes.
- Vendor supplied passwords shall be changed immediately upon installation.
- Temporary passwords shall be changed on first use of the system.
- Passwords, along with hints and reminders, shall be stored in protected, encrypted files.
- Applicable devices and application systems shall maintain a password history file, where the capability exists, to prevent continual reuse of the same password for a valid userID.

4.1.2. Kerberos - A secure method for authenticating a request for a service in a computer network. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server. It shall be based on symmetric

cryptography, so the user's password does not actually pass through the network as plain text.

4.1.3. Personal Identification Number (PIN) - A character string used as a password to gain access to a system resource. PINs shall only be entered using a keypad and usually not sent across the network, to prevent interception. PINs may be used in conjunction with other types of authentication devices (i.e., a smart card).

4.2 AUTHENTICATION BY OWNERSHIP – User authentication shall be based on something only the user possesses, making it more secure than a knowledge-based system, and may include the following:

Hardware Based Challenge-Response – The server challenges the user to demonstrate that he/she possesses a specific token and knows the PIN or passphrase by combining them to generate a response that is valid, but only once. This includes but is not limited to:

- A small, handheld device, with or without a key pad, containing an LCD window or display interface – the device acts as the user's token.
- A proximity token where a user wears the token on their person. The token automatically logs out the user or locks the client device when the user gets "too far" away from the device. To be used with a password for strong authentication.
- A smart card. An International Organization for Standardization (ISO) 7816-compliant chip card with CPU and memory. Contact smart cards require PC/SC standard readers, based on ISO 7816, and supporting workstation software. Contactless smart cards require a Mifare architecture card reader based on ISO Standard 14443A.
- A Universal Serial Bus (USB) key. A device with CPU memory that plugs into a universal serial bus port on a workstation.
- A Bluetooth-enabled token with CPU and memory. Bluetooth is a short-range, 2.45GHz wireless connection protocol.

Symmetric-Key Cryptography - A cryptographic system in which the sender and receiver of a message share a single, common key used to encrypt and decrypt the message. (Reference Statewide Standard P800-S850, Encryption Technologies.)

Asymmetric-Key Cryptography - A cryptographic system that uses two keys, a *public key* known to everyone and a *private* or *secret key* known only to the recipient of the message. (Reference Statewide Standard P800-S850, Encryption Technologies.)

4.3 AUTHENTICATION BY CHARACTERISTIC – User authentication based on information about a person gathered by digitizing measurements of a

physiological or behavioral characteristic has been categorized as an emerging technology. When used, implementations shall be based on open, industry standards, if available. Requirements may be issued for the following areas once the technology matures to the point of becoming strategic for the State:

Physiological characteristic such as:

- Fingerprint – any fingerprint imaging used shall conform to current Department of Public Safety (DPS) Fingerprint Imaging Bureau standards.
- Iris patterns.
- Retina patterns.
- Hand geometry.
- Face geometry.
- Palm print.

Behavioral characteristics such as:

- Voiceprint (speech patterns).
- Signature.
- Keystroke dynamics.

4.4 DIRECTORY SERVICES - Lightweight Directory Access Protocol (LDAP) shall be used to provide access to directory and application services.

- LDAP is the lightweight version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.
- As a widely accepted industry standard for access to directory information, LDAP supports multi-vendor interoperability by providing an open, extensible, vendor-independent, platform-independent, protocol standard.
- LDAP directories provide repositories for security-related data (e.g., userIDs, passwords, URLs, pointers, binary data, Public Key Certificates, etc.).
- The LDAP protocol directly supports various forms of strong security technology used to perform authentication, privacy, and data integrity services.
- The LDAP Version 3 proposal for Transport Layer Security (TLS) includes data encryption methods.
- LDAP supports the use of Directory Services Markup Language (DSML)v2 and Simple Object Access Protocol (SOAP) to allow LDAP directory information to be expressed in a common format and transmitted beyond the traditional firewall and into Internet-based applications.
- LDAP supports the use of the open, industry standard Java Naming and Directory Interface (JNDI) for directory access and support.
- LDAP supports the use of the Security Assertion Markup Language (SAML) standard as an authentication protocol that may be used between Web servers for federated affiliation.

- The Directory Enabled Networking (DEN) and Common Information Model (CIM) XML-based, industry-standard initiatives are being mapped into the LDAP directory structure. CIM is more comprehensive than the Desktop Management Interface (DMI) model and can be used in conjunction with the Simple Network Management Protocol (SNMP).
- Future meta-directory services should be established with individual LDAP directory repositories and be accessible via standard LDAP protocols. Meta-directory service design should include obtaining an Object Identifier (OID) tree for the State from the Internet Assigned Numbers Authority (IANA) that can be used to uniquely identify attributes and object classes to facilitate the matching and coordination of information among individual LDAP implementations.

4.5 ACCESS TO RESOURCES AND SERVICES – shall be in accordance with Statewide Standard P800-S885, IT Physical Security, Statewide Standard P800-S890, Personnel Security, and Statewide Standard P800-S810, Account Management. Internal and external connectivity to networks to provide access to resources and services shall be in accordance with Statewide Standard P800-S830, Network Security.

4.6 MOBILE/EXTERNAL AUTHENTICATION
Mobile/External connections to networks, in accordance with Statewide Standard P800-S830, Network Security, shall be routed through secure gateways, encrypted, and require a two factor strong authentication which is something the user has and something the user knows.

Such strong authentication methods can be challenge response devices, one-time passwords, additional PIN, token based authentication, Kerberos, smart cards, key fobs, USB dongles, as well as the standard method of authentication required by the budget unit for internal connectivity (commonly referred to as multifactor authentication.)

Budget unit authentication methods shall be documented and maintained as part of, and in accordance with, Statewide Standard P800-S810, Account Management.

5. DEFINITIONS 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.
    6.16.1. Statewide Standard P800-S810, Account Management.
    6.16.2. Statewide Standard P800-S830, Network Security.
    6.16.3. Statewide Standard P800-S850, Encryption Technologies.
    6.16.4. Statewide Standard P800-S885, IT Physical Security.
    6.16.5. Statewide Standard P800-S890, Personnel Security.
6.17. State of Arizona Target Security Architecture, http://www.azgita.gov/enterprise_architecture.

7. ATTACHMENTS

None.

About GITA

IT Coordination and Planning
Statewide Plan and Applications
Enterprise Architecture
Service Oriented Architecture
Policies, Standards, Procedures

IT Project Review and Monitoring
Project Investment Justification
Project Oversight
Project Management Certification

E-Government

Information Security and Privacy
Incident Response
Security Practitioner Certification

Public Safety Communications

Strategic Initiatives

Telecommunications

Councils and Committees

Policies, Standards, and Procedures (PSP)

Statewide IT Policies, Standards, and Procedures are based on Enterprise Architecture (EA) strategies and framework. The purpose of EA is to provide a comprehensive framework of business principles, best practices, technical standards, migration and implementation strategies, that direct the design, deployment and management of information technology (IT) for the state agencies. More information about EA is available in P700 Enterprise Architecture Policy.

PSP Vision, Mission, Principles, and Goals

Contact

RAJ Kollengode
Head of Enterprise Architecture and Strategy
602-364-4790

PSP Forms

Online Non-Disclosure Agreement

PSP Categories:

- Management Practices
- Web Services
- IT Enterprise Architecture
- Security

Glossary of Terms: Policies, Standards and Procedures and Enterprise Architecture

Management Practices:

P100 - Statewide Information Technology Policy	doc	pdf
P105 - Policies, Standards, and Procedures (PSP) Policy	doc	pdf
•S105 - PSP Standard	doc	pdf
•P105 - GITA PSP Procedures	doc	pdf
P136 - IT Planning Policy	doc	pdf
P140 Web Conferencing	doc	pdf
P150 Virtual Office Policy	doc	pdf
P335 - Project Management Certification Policy	doc	pdf
P340 - Project Investment Justification (PIJ) Policy	doc	pdf
•S340 - Project Investment Justification (PIJ) Standard	doc	pdf
•P340 - GITA PIJ Procedure	doc	pdf
•S341 - Project Status Reporting (PIJ) Standard	doc	pdf
•S342 - Request for Special Funding (PIJ Projects) Standard	doc	pdf
•S343 - Project Oversight Standard	doc	pdf

Go to top

Web Services:

P125 - Web Portal Acceptable Use Policy	doc	pdf
P130 - Web Site Accessibility Policy	doc	pdf
P170 - Privacy Policy	doc	pdf
P252 - Intellectual Property Policy	doc	pdf
P350 - Web Related Development - Notice of Intent (NOI)	doc	pdf
P401 - Email Use Policy	doc	pdf
P501 - Internet Use Policy	doc	pdf
P505 - Social Networking Policy	doc	pdf

Go to top

IT Enterprise Architecture:

P700 - Enterprise Architecture Policy	doc	pdf

P710 - Network Architecture Policy	doc	pdf
•S710 - Network Infrastructure Standard	doc	pdf
P720 - Platform Architecture Policy	doc	pdf
•S720 - Platform Infrastructure Standard	doc	pdf
P730 - Software Architecture Policy	doc	pdf
•S730 - Applications and Related Software Standards	doc	pdf
•S731 - Software Productivity Tools Standard	doc	pdf
P740 - Data/Information Architecture Policy	doc	pdf
•S740 - Data Modeling Standard	doc	pdf
•S741 - Classification and Categorization of Data Standard	doc	pdf
•S742 - Database Access Standard	doc	pdf
P750 - Service Oriented Architecture Policy	doc	pdf

Go to top

Security:

P800 - IT Security Policy	doc	pdf
•S805 - IT Risk Management Standard	doc	pdf
•S810 - Account Management Standard	doc	pdf
•S815 - Configuration Management Standard	doc	pdf
•S820 - Authentication and Directory Services Standard	doc	pdf
•S825 - Session Controls Standard	doc	pdf
•S830 - Network Security Standard	doc	pdf
•S850 - Encryption Technologies Standard	doc	pdf
•S855 - Incident Response and Reporting Standard	doc	pdf
•S860 - Virus and Malicious Code Protection Standard	doc	pdf
•S865 - IT Disaster Recovery Planning (DRP) Standard	doc	pdf
•S870 - Backups Standard	doc	pdf
•S875 - Maintenance Standard	doc	pdf
•S880 - Media Sanitizing/Disposal Standard	doc	pdf
•S885 - IT Physical Security Standard	doc	pdf
•S890 - Personnel Security Standard	doc	pdf
•S895 - Security Training and Awareness Standard	doc	pdf

Go to top

E-Government Services

The Digital Government Services Division within GITA is responsible for developing strategies and deploying accessible, reliable and cost-effective digital government services to Arizona government entities. A full complement of services is available to meet the requirements of large and small agencies.

The centerpiece of GITA's e-Government service offering is the State of Arizona web portal, www.AZ.gov. With oversight and management provided by GITA, the State web portal provides application development, web site development, hosting and support services for State and local government agencies.

Additional GITA e-government services include digital government readiness consultation, extensive webmaster tools, .gov domain registration and a Notice of Intent (NOI) approval process for agency web-based initiatives.

State of Arizona Web Portal

The State of Arizona Web Portal, www.AZ.gov, is an award-winning web site providing citizens, businesses and other government entities with faster, easier and more intuitive access to government. In addition to providing a convenient one stop access to government information the State web portal provides custom application development, web site development, hosting and support services for State and local government agencies. Through a unique funding model the portal is often able to underwrite the costs associated with these services. Approximately 75 agencies, boards and commissions utilize at least one service offered by the portal.

The portal is a key enabler to accelerate and enhance the on-line presence of any agency. Applications specializing in the following disciplines have been developed and deployed.

- Licensing and permitting
- Inter/intra-governmental data sharing
- Public access to government information
- Core utility services such as:

  - • Credit card processing capabilities that are seamlessly integrated with the State accounting system,
    • A secure access control component that supports easily integrates with almost any web-based application,

    • GIS (Geographic Information Systems) processing and,
    • A custom Google search engine appliance that can be easily integrated into an agency's existing web site.

These and other infrastructure components provide agencies with the ability to develop applications without the additional development and maintenance costs associated with such services. This common infrastructure simplifies the development, implementation and maintenance of online services - ultimately resulting in costs-savings to agencies.

The State has selected NIC, Inc (www.nicusa.com) to manage the web portal under contract EPS070078-1-A1. The web portal contract provides a solid foundation for agencies to deliver leading e-government applications and services to their constituents.

Services

State of Arizona Web Portal
Digital Government Readiness Consultation
.gov Domain Registration
Webmaster Tools
Notice of Intent (NOI) Process
AZ3D

AZ.GOV
Arizona's Official Web Site
Website Redesign Project

Contact

Andy Miller
Manager Digital Government Services
State Web Portal Manager
602-364-4788

Shanna Anderson
Web Content Coordinator
(602) 284-9005

Using the Contract:

1. The agency contacts the State Web Portal Manager to discuss contract applicability for the request,

2. A requirements review is conducted:

   - Meet with the agency customer to identify and clarify the requirements,

3. NIC issues a project charter:

   - Identify costs (if any), hours, roles, deliverables, etc.
   - Obtain approval from Agency and GITA,

4. Work begins!

Top

Digital Government Readiness Consultation

GITA works with agencies to move their business processes on-line. Agencies interested in moving a business function on-line must consider potential impact from multiple perspectives. Many functions at any given agency are candidates for e-enablement and some projects require a minimal amount of effort and return a significant amount of customer satisfaction and/or agency savings. GITA and the State web portal vendor can provide assistance by offering lessons learned from other e-government projects. Because Arizona's web portal vendor operates web portals for twenty other states they have a significant knowledge base of best practices and successful projects implemented across the country. Contact the GITA Digital Government Services Manager for more information.

.gov Domain Registration

In an effort to standardize web and e-mail addresses, State agencies are encouraged to move to a second level .gov domain name. This assures citizens that they are accessing official government websites, and often times, the website address is shorter and more recognizable.
Examples: azdes.gov, azag.gov, azgita.gov, etc.

Top

Webmaster Tools

GITA provides assistance for agencies to meet State standards for website development. Website redesign information is available to ensure common look and feel among agency websites. There are several web standards and policies in place that provide direction on achieving a common look and feel and to incorporate website accessibility and usability. GITA offers a Google search appliance for agency use at no cost that provides users with a trusted tool for finding information quickly. Webmaster assistance is offered to help achieve the State's standards. As needed, ongoing education and outreach is provided to share information, and provide training and additional tools that will help agencies meet their website development goals.

Top

Notice of Intent (NOI) Process

The NOI process is intended to ensure that agencies are employing cost efficient means in deploying all web-related services, evaluating the

services offered through the AZ.gov Portal, adhering to statewide P350 NOI policy as published and maintaining a consistent look and feel in their website designs. An NOI must always be submitted to and reviewed by GITA before any money is expended on web development.

Top

AZ3D

GITA, in partnership with the Arizona Department of Homeland Security and other state agencies, is researching the feasibility of creating a statewide visualization platform for Arizona. This system would integrate imagery and numerous datasets with geo-based attributes into a non-technical internet-based viewing environment – or 'common operating picture.' When integrated and displayed in a virtual environment, these datasets can be shared and utilized by state and local government emergency planners, first responders and other decision makers.

Key Partners - **Arizona Department of Homeland Security**

For more information – **Brian Sherman**

Top