

ARKANSAS REGISTER

Proposed Rule Cover Sheet



Secretary of State
John Thurston
500 Woodlane Street, Suite 026
Little Rock, Arkansas 72201-1094
(501) 682-5070
www.sos.arkansas.gov



Name of Department _____

Agency or Division Name _____

Other Subdivision or Department, If Applicable _____

Previous Agency Name, If Applicable _____

Contact Person _____

Contact E-mail _____

Contact Phone _____

Name of Rule _____

Newspaper Name _____

Date of Publishing _____

Final Date for Public Comment _____

Location and Time of Public Meeting _____

FINANCIAL IMPACT STATEMENT

PLEASE ANSWER ALL QUESTIONS COMPLETELY.

DEPARTMENT _____
BOARD/COMMISSION _____
PERSON COMPLETING THIS STATEMENT _____
TELEPHONE NO. _____ **EMAIL** _____

To comply with Ark. Code Ann. § 25-15-204(e), please complete the Financial Impact Statement and email it with the questionnaire, summary, markup and clean copy of the rule, and other documents. Please attach additional pages, if necessary.

TITLE OF THIS RULE _____

1. Does this proposed, amended, or repealed rule have a financial impact?
Yes No

2. Is the rule based on the best reasonably obtainable scientific, technical, economic, or other evidence and information available concerning the need for, consequences of, and alternatives to the rule?
Yes No

3. In consideration of the alternatives to this rule, was this rule determined by the agency to be the least costly rule considered? Yes No

If no, please explain:

(a) how the additional benefits of the more costly rule justify its additional cost;

(b) the reason for adoption of the more costly rule;

(c) whether the reason for adoption of the more costly rule is based on the interests of public health, safety, or welfare, and if so, how; and

(d) whether the reason for adoption of the more costly rule is within the scope of the agency's statutory authority, and if so, how.

4. If the purpose of this rule is to implement a *federal* rule or regulation, please state the following:
(a) What is the cost to implement the federal rule or regulation?

Current Fiscal Year

General Revenue _____
 Federal Funds _____
 Cash Funds _____
 Special Revenue _____
 Other (Identify) _____

Total _____

Next Fiscal Year

General Revenue _____
 Federal Funds _____
 Cash Funds _____
 Special Revenue _____
 Other (Identify) _____

Total _____

(b) What is the additional cost of the state rule?

Current Fiscal Year

General Revenue _____
 Federal Funds _____
 Cash Funds _____
 Special Revenue _____
 Other (Identify) _____

Total _____

Next Fiscal Year

General Revenue _____
 Federal Funds _____
 Cash Funds _____
 Special Revenue _____
 Other (Identify) _____

Total _____

5. What is the total estimated cost by fiscal year to any private individual, private entity, or private business subject to the proposed, amended, or repealed rule? Please identify those subject to the rule, and explain how they are affected.

Current Fiscal Year

\$ _____

Next Fiscal Year

\$ _____

6. What is the total estimated cost by fiscal year to a state, county, or municipal government to implement this rule? Is this the cost of the program or grant? Please explain how the government is affected.

Current Fiscal Year

\$ _____

Next Fiscal Year

\$ _____

7. With respect to the agency's answers to Questions #5 and #6 above, is there a new or increased cost or obligation of at least one hundred thousand dollars (\$100,000) per year to a private individual, private entity, private business, state government, county government, municipal government, or to two (2) or more of those entities combined?

Yes No

If yes, the agency is required by Ark. Code Ann. § 25-15-204(e)(4) to file written findings at the time of filing the financial impact statement. The written findings shall be filed simultaneously with the financial impact statement and shall include, without limitation, the following:

- (1) a statement of the rule's basis and purpose;
- (2) the problem the agency seeks to address with the proposed rule, including a statement of whether a rule is required by statute;
- (3) a description of the factual evidence that:
 - (a) justifies the agency's need for the proposed rule; and
 - (b) describes how the benefits of the rule meet the relevant statutory objectives and justify the rule's costs;
- (4) a list of less costly alternatives to the proposed rule and the reasons why the alternatives do not adequately address the problem to be solved by the proposed rule;
- (5) a list of alternatives to the proposed rule that were suggested as a result of public comment and the reasons why the alternatives do not adequately address the problem to be solved by the proposed rule;
- (6) a statement of whether existing rules have created or contributed to the problem the agency seeks to address with the proposed rule and, if existing rules have created or contributed to the problem, an explanation of why amendment or repeal of the rule creating or contributing to the problem is not a sufficient response; and
- (7) an agency plan for review of the rule no less than every ten (10) years to determine whether, based upon the evidence, there remains a need for the rule including, without limitation, whether:
 - (a) the rule is achieving the statutory objectives;
 - (b) the benefits of the rule continue to justify its costs; and
 - (c) the rule can be amended or repealed to reduce costs while continuing to achieve the statutory objectives.

~~DRAFT~~ Standard Statement – Encryption

~~Title:~~ Encryption

~~Document Number:~~ SS-70-006

~~Effective Date:~~ Upon the earlier of: 1) July 1, 2008; or
2) The line-item appropriation to the agency in question of
funds to comply with the rule

~~Published by:~~ Office of Information Technology

~~1.0 Purpose~~

~~Sensitive information held by public organizations can include social security numbers, credit card numbers, and other personal information about Arkansas' citizens. Government, in particular, is responsible for information that protects public health and public safety. Individuals with malicious intent can easily acquire information being transmitted electronically unless appropriate security measures are applied, such as encryption.~~

~~If detected, the credentials employees use to access data and systems can provide unauthorized access which can lead to critical data being modified, deleted and ultimately made unavailable. For these reasons very sensitive information must be protected through encryption methods.~~

~~2.0 Scope~~

~~This standard statement applies to all state agencies, administrative portions of institutions of higher education, boards and commissions.~~

~~3.0 Background~~

~~The Arkansas Information Systems Act of 1997 (Act 914, 1997) gives the Office of Information Technology the authority to define standards, policies and procedures to manage the information resources within the state. This is accomplished through work with a multi-agency working group known as the Shared Technical Architecture Team.~~

~~In addition, Act 1042 of 2001 states that the Executive Chief Information Officer oversees the development of information technology security policy for state agencies, boards and commissions and administrative portions of institutions of higher education.~~

~~4.0 References~~

~~4.1~~ — ~~Act 914 of 1997: Authorized the Office of Information Technology (OIT) to develop statewide policies.~~

~~4.2~~ — ~~Act 1042 of 2001: Authorized the Executive CIO to develop security policy.~~

5.0 — Standard

- 5.1** — The following standard applies only to data that is classified by the SS-70-001 [Data and System Security Classification Standard](#) as being Level C — Very Sensitive or Level D — Extremely Sensitive and transmitted on a public network, including the state network, or removed from a covered entity's physical location
- 5.1.1** — Users accessing data from outside organizational local area networks must encrypt their credentials, including login IDs and passwords, to access such data.
- 5.1.2** — Data on all portable media and electronic devices, such as laptops, PDAs, flash drives, CDs, DVDs, or any external storage device shall be encrypted. Compliance by covered entities with Section 5.1.2 shall be achieved upon the earlier of: 1) July 1, 2008; or 2) The line item appropriation to the agency in question of funds to comply with the rule.
- 5.1.3** — Backups for business continuity purposes that are taken offsite shall be encrypted. Compliance by covered entities with Section 5.1.3 shall be achieved upon the earlier of: 1) January 1, 2009; or 2) The line item appropriation to the agency in question of funds to comply with the rule.
- 5.1.3.1** — Archived backups created prior to the effective date of this standard are exempt from this encryption requirement and are subject to the requirements of the Physical and Logical Security Standard (SS-70-008).
- 5.1.3.2** — Encryption keys used to encrypt data used for business continuity purposes must be stored offsite within a locked or otherwise restricted environment in a building. Data shall be encrypted with algorithms utilizing 128 bit encryption, at a minimum.
- 5.1.4** — Acceptable methods of 128 bit or higher encryption include, *but are not limited to*:
- 5.1.4.1** — Triple-DES
- 5.1.4.2** — Advanced Encryption Standard
- 5.1.4.3** — International Data Encryption Algorithm (IDEA)
- 5.1.4.4** — RSA (key length must be 1024 bits or higher)
- 5.1.4.5** — SSL (secure socket layer)
- 5.1.5** — Unacceptable encryption methods include, *but are not limited to*:
- 5.1.5.1** — DES (Data Encryption Standard)
- 5.1.6** — Encryption shall be used for data transmissions such as FTP (file transfer protocol) and Telnet. Methods of acceptable encryption include, but are not limited to, SSH, third party secure FTP solutions, and the use of a virtual private network.

6.0 — Procedures

The State Security Office reserves the right to audit for compliance with this standard. Furthermore, the State Security Office has the right to grant an exception or exclusion to any part of this standard. With thirty days written notice, the State Security Office reserves the right to update the unacceptable encryption methods list as defined in Sections 5.1.5.

Covered entities may request an extension to come into compliance with any part of this standard by contacting the State Security Office with an expected compliance date. The State Security Office must approve all extension requests.

7.0—Revision History

Date	Description of Change
xx/xx/2006	Original Standard Statement Published

8.0—Definitions

8.1—Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is an encryption algorithm utilizing the Rijndael specification for securing information by federal government agencies. Key sizes of 128, 192, and 256 bits are specified in the AES standard. AES was approved by the National Institute of Standards and Technology (NIST) as US FIPS PUB 197.

8.2—Backup

Information archived for the purpose of recovering systems and data in the event of a disaster or loss of data.

8.3—Data Encryption Standard (DES)

The Data Encryption Standard is a symmetric key algorithm adopted by the federal government as a federal standard for protecting sensitive unclassified information. With an effective key length of 56 bits, DES was compromised in 1997.

8.4—File Transfer Protocol (FTP)

An application layer protocol that uses Transmission Control Protocol (TCP) and telnet services to transfer bulk data files between machines or hosts.

8.5—Flash drive

Flash drives, also referred to as thumb drives or USB drives, are portable storage devices that use flash memory and are very lightweight and small. Flash drives can be used in place of a floppy disk, zip drive disk, or CD.

8.6—Personal Digital Assistant (PDA)

A PDA is a small handheld device that combines computing, information storage, telephone, fax, and Internet.

8.7—RSA

The RSA algorithm, developed by Rivest, Shamir and Adleman, can be used for public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.

8.8—Secure Shell (SSH)

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer. Both ends of the client/server connection are authenticated using a digital certificate and passwords are encrypted. SSH uses RSA public key cryptography for both connection and authentication. SSH 1 is considered obsolete as it is susceptible to man-in-the-middle attacks. SSH 2 replaces SSH 1.

8.9—Secure Socket Layer (SSL)

SSL is a protocol uses the public and private key encryption system, which also includes the use of a digital certificate. SSL is an integral part of most Web browsers (clients) and Web servers.

8.10 Telnet

Telnet is a network protocol that is used to connect to remote computers for the purpose of executing commands on a remote machine. Telnet is considered to be insecure due to several well known vulnerabilities.

8.11 Triple DES Encryption

Triple DES encryption encrypts data using the DES algorithm three times. Three 56-bit keys are used, instead of one, for an overall key length of 192 bits.

8.12 Secure Virtual Private Network (VPN)

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

9.0 Related Resources

9.1 Data and System Security Classification Standard:

<http://www.cio.arkansas.gov/techarch/indexes/standards.htm>

9.2 Physical and Logical Security Standard:

<http://www.cio.arkansas.gov/techarch/indexes/standards.htm>

9.3 COBIT standards:

www.isaca.org/cobit.htm

9.4 Act 1526 of 2005:

<http://www.arkleg.state.ar.us/acts/2005/public/Act1526.pdf>

9.5 HIPAA Security Standards:

<http://www.hipaadvisory.com/regs/finaalsecurity/>

10.0 Inquiries

Direct inquiries about this standard to:

Office of Information Technology

Enterprise Architecture

124 West Capitol Avenue Suite 990, Little Rock, Arkansas 72201

Phone: 501-682-4300

FAX: 501-682-2040

Email: sharedarchitecture@arkansas.gov

OIT standards, policies and best practices can be found on the Internet at:

<http://www.cio.arkansas.gov/techarch>

Jennifer Davis

From: Legal Ads <legalads@arkansasonline.com>
Sent: Thursday, December 26, 2024 12:00 PM
To: Jennifer Davis
Subject: Re: Notice of Rulemaking

Will run Sat 12/28, Sun 12/29, and Mon 12/30/

Thank you,

Gregg Sterne, Legal Advertising
Arkansas Democrat-Gazette
legalads@arkansasonline.com

From: "Jennifer Davis, DIS" <Jennifer.Davis@arkansas.gov>
To: "legalads" <legalads@arkansasonline.com>
Sent: Thursday, December 26, 2024 11:50:32 AM
Subject: Notice of Rulemaking

Greetings,

Please run the attached Notice of Rulemaking for 3 consecutive days as soon as possible to include Sunday as one of the three days. The billing address is the Arkansas Department of Transformation and Shared Services, PO Box 3522, Little Rock, AR 72203. If you have any questions, please contact me at 501-683-1672.

Please confirm the dates in which the notice will run.

Thank you,
Jennifer



Jennifer Davis
Chief Privacy Officer
Transformation and Shared Services
E: Jennifer.Davis@arkansas.gov
O: 501-683-1672

Notice of Rulemaking

Pursuant to Arkansas Code Annotated § 25-15-201 et seq., notice is hereby given that the Arkansas Department of Transformation and Shared Services, Division of Information Systems is considering a repeal of the following rules: (1) Policy Statement – Project Management; (2) Standard Statement – Password Management; (3) Standard Statement – Virus Scanning; (4) Standard Statement – Warning Banner; (5) Standard Statement – Personnel Security; (6) Standard Statement – Encryption; and (7) Department of Information System Rules dated October 17, 1997. A public hearing will be held on January 21, 2025, at 1:30pm in the River Valley Conference Room, 501 Woodlane Avenue, Suite G-08, Little Rock, AR 72201. Written comments should be mailed to TSS, Attn: Public Comments at P.O. Box 3522, Little Rock, AR 72203. Comments may also be e-mailed to TSS.RulesComments@arkansas.gov. Copies of the proposed rule may also be obtained from the Department of Transformation and Shared Services, 501 Woodlane Avenue, Little Rock, AR 72201, or by accessing the Department's website at <https://transform.ar.gov/secretarys-office/legal/rules-hearings/>.