

# State Security Office

## Financial & Risk Impact Statement for Proposed Encryption Standard

### The Major Requirements of the Encryption Standard

- **Requires** encryption of transmitted data that is classified by the [Data and System Security Classification Standard](#) (SS-70-001) as Level C (Very Sensitive) or Level D (Extremely Sensitive)
- **Does not require** encryption of databases within agencies
- **Requires** encryption of very sensitive and extremely sensitive information on electronic media leaving the organization such as thumb drives, laptops and DVDs
- **Requires** encryption of backups containing Level C and Level D data that are taken off site

[ [View the Draft Encryption Standard](#) ]

Before promulgating standards, it is important to ascertain the impact to the organizations subject to the standard. Please fill out the following impact statement for the Encryption Standard proposed by the Arkansas State Security Office.

<b>Organization/School Name</b>	
<b>Division</b>	
<b>Person completing this statement</b>	
<b>Telephone number</b>	
<b>Email address</b>	

1. If your organization is considering changing business processes or practices (work flow) in order to meet this standard, how will it be done?
  - Not housing information classified by the *Data and System Security Classification Standard (SS-70-001)* as Level C Very Sensitive or Level D Extremely Sensitive on a PDA, laptop, or other mobile device
  - Outsourcing transactions dealing with sensitive information to third parties for processing (for example, INA handling online processing of credit card transactions)
  - Reduction, delay or elimination of existing or planned services (for example, your organization was planning on offering the ability to accept payment or sensitive information online, but now you aren't.)
  - Other (please describe)
2. If your organization is considering changing organization policies in order to meet this standard, how will it be done?
  - Our organization will not allow employees to remove information classified by the *Data and System Security Classification Standard (SS-70-001)* as Level C Very Sensitive or Level D Extremely Sensitive in electronic form from the organization.
  - Our organization will require employees removing information classified by the *Data and System Security Classification Standard (SS-70-001)* as Level C Very Sensitive or Level D Extremely Sensitive from the organization to encrypt the information.
  - Other (please describe)
3. Do you believe this proposed standard will bear a financial cost upon your organization or your customers?  
Check one: No  (if "No", go to **Question 7**)    Yes  (if "Yes", **please continue**)

4. Please estimate the financial cost by fiscal year of implementing this proposed standard:  
(please indicate the first fiscal year)

First Fiscal Year:

- a. Staff time cost:
- b. Money outlay (programming costs, purchase of equipment/software, etc.):
- c. Training:
- d. Customer cost:
- e. Other resource cost (Please explain):

5. Is this a recurring cost for more than one fiscal year? No  Yes

6. If the cost will be more for successive years, please indicate your estimates:

Fiscal Year:

- a. Staff time cost:
- b. Money outlay (programming costs, purchase of equipment/software, etc.):
- c. Training:
- d. Customer cost:
- e. Other resource cost (Please explain):

Fiscal Year:

- a. Staff time cost:
- b. Money outlay (programming costs, purchase of equipment/software, etc.):
- c. Training:
- d. Customer cost:
- e. Other resource cost (Please explain):

7. Does this standard pose a conflict with your current technology?

No

Yes  If "Yes" please explain:

8. Does this standard lower your risk of breaching sensitive information?

No

Yes  If "Yes" please explain:

9. Would this impact any partnerships or consortiums your organization is involved in?

No

Yes  If "Yes" please explain:

10. Does this impact your ability to provide any other government service?

No

Yes  If "Yes" please explain:

11. How many people are employed by your organization?

12. What number of employees would be impacted by this standard?

13. For how many individuals do you maintain very sensitive or extremely sensitive information that would be impacted by this standard?

14. For how many other entities (businesses, organizations, etc.) do you maintain very sensitive or extremely sensitive information that would be impacted by this standard?

15. Do you have any comments about the proposed encryption standard?

16. How much storage space is required to do a complete backup of all your organization's data?