

**Minutes from Meeting on February 13, 2008**

**Meeting called to order:** 1:30 PM at the Judicial Building

**Persons in attendance:**

John Wolf ILOT	Don Harvey IVH
Alison Radl DAS-ISO	Ruth Coleman DRF
Calvin Moore DAS-ISO	Diana Thompson IWD
Mike Chesmore DAS-ISO	Deb Castillo IVRS
Evelyn Halterman ILOT	Jeff Franklin DNR
Haider Qleibo DNR	Debra Covington DOT
Linda Torgeson DOT	Greg Fay DAS-ISO
Shane Ludwig IUB	Doug Douty JB
Verne Logan IDOM	Dave Kair LSA

**Agenda**

**Enterprise Standards/Polices: Enterprise Security Standard/Mobile Device Standard/Data Stewardship Standard/Removable Storage Policy//Data Classification/Laptop Encryption**

**Projects: Executive IT Security Briefing/any others?**

**NASCIO At Risk video viewing**

**Meeting Points**

**Enterprise Policies & Standards**

The Enterprise Security Standard and the Mobile Device Security Standard – going to TGB - IT Standard Advisory Group March 6 meeting for comments and/or approval

**Data Stewardship Standard**

- 1. Change Steward to Steward(s)
- 9. Standard was developed to the cover the basics of data collection – trying to protect privacy – if you don't need the data don't collect it particularly confidential data, i.e. social security numbers. If your agency has a strong business need or argument then it's okay.
- 10b: Develop a written policy covering data sharing. Suggested to change to written and signed.
- Trying to make minimum standard – the standard does not decide your agency mission.
- 13. Why 20 days for the notification period? Originally it was 10 days but an agency suggested going to 20. Discussion about the public's perception of data breaches. The notification provision was changed to match House Study Bill 617.

Notification: State agencies shall notify customers affected by a data breach. Notice shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach of security and with the legitimate needs of law enforcement.

- **Please look through the updated standard and submit any comments/suggestions to Alison through the middle of March**

*Question – who at your agency is your ‘data steward(s)? Are they technical staff or non-technical?*

### **ISO – Policies/Standards; Removable Storage Policy/Data Classification/Laptop Encryption**

- Data Classification – ongoing - If you have not already done so please email your agency’s status to [Greg.Fay@iowa.gov](mailto:Greg.Fay@iowa.gov)
- Laptop Encryption – ongoing - Most agencies are working on complying with this standard. The TGB is very interested in agencies complying with this standard.
- Removable Storage Encryption – compliance extended to March 31, 2008

Administrative Rule of Policy Compliance is that the CIO can request extra time. The dates for compliance are on the intranet site with each policy/standard. If there has been a state wide extension granted, Greg Fay will send an email to the CIOs.

### **Intranet and ISO Internet Sites**

More information has been put on the site. Effort was made to make it more organized. Also included are training courses available. There is more on resources and training development.

ISO internal site - <http://intranet.iowa.gov/iso/index.html>

ISO external site - <http://secureonline.iowa.gov/>

**Please email a copy of your department’s security policy to Alison ([alison.radl@iowa.gov](mailto:alison.radl@iowa.gov)).**

Here is the link where the new policies/standards are: .

[http://das.ite.iowa.gov/standards/enterprise\\_it/index.html](http://das.ite.iowa.gov/standards/enterprise_it/index.html)

Only the standards that are passed by the TGB are on the ISO site. Alison will send out all three draft standards with a watermark of “DRAFT” and date revised.

### **Executive IT Security Briefing project**

Need volunteers to help out with the video shoot. The highlighted sections are where we need to shoot some video and we’re looking for several agencies to participate. (see attached)

Some of the concepts could be changed; we’re just looking for something that works for that section of the script.

### **Feedback/input/information regarding security**

Concerns about application security – some agencies are looking at 3<sup>rd</sup> party applications – what kind of security standard do they have?

It’s hard to develop an enterprise application security standard. OSWASP site provides guidelines on application development. It was asked if ITE has some best practices or standards. It would be nice to have a document that outlines the top 10 best practices.

### **Open Discussion**

ISO Risk Assessments are being scheduled with agencies. It’s a review from last year. Also may talk a little about your agency and the Enterprise Standards.

**Meeting Adjourned: 3:00 P.M.**

**Next Meeting:** February 13, 2008 1:30 P.M. – 3:00 P.M.