



IS Council Meeting Summary

August 16, 2010

12pm – 2pm

COV IS Council members attending:

**Goran Gustavsson (APA)
Ed Miller (DOA)
John Green (VITA ex-officio)**

**David Hines (SCV)
John Willinger (DBHDS)**

COV IS Council Members attending via teleconference:

**Andy Hallberg (ABC)
Michael McDaniel (VRS)
Todd Richardson (DMME)**

**Doug Mack (DMV)
Shirley Payne (UVA)**

COV IS Council members absent:

Sandra Graham (Chest. Cty)

Also attending: Norm Hill (DMV)

Encryption Committee Report – David Hines, SCV

Committee has no updates at this time, however, the Committee is making progress and will have 3 documents to present soon. All documents revolved around 'Best Practices'.

WebApps Committee Report – John Willinger, DBHDS

Committee is working on best practices/guideline documents. Committee will have documents ready for distribution by October IS Council meeting to be used for Cyber Security Awareness Month.

Making IT Security an Executive Management Priority Committee Report – John Green, VITA

Committee will hold meeting today and begin working on some new leadership communications to support ISO's.

Risk Management Committee – Ed Miller, DOA

Committee has met with IREC and recently had a software demo. Both of which were beneficial. Committee will begin focusing on short term deliverables for December 2010 time frame involving questionnaires around risk profiles of agencies.

Open Web App Security Program (OWASP) – Todd Richardson (DMME)

Todd expressed the need for a web apps standard or baseline testing to meet some level of security assurance in the Commonwealth. He added that it should include external, internal and third party applications. Ed added that he would like to see a certification process via a Standard. Discussion surrounding the need and development of such a standard followed. WebApps Committee will include OWASP in their discussions.

SEC502-Audit Requirements – Ed Miller (DOA)

Ed explained that the Standard is unclear as far as what is expected regarding who will perform an agency's audit of their sensitive systems. He added that a concern is also involved on where an agency's sensitive system resides and what level of risk is associated with the system. Ed suggests that a tool be developed for lower risk systems and use an outside source for higher risk systems. John Green stated that he understands there are serious concerns as a consensus however, due to budgetary constraints in the Commonwealth we will have to rely on internal audit at the agencies.

Other business

David presented Council members with a few items for open discussion. David requested the status of any proposed or new standards or policies. John Green explained all current proposed standards and policies are on ORCA for comment and review. John also explained that prior to publishing of any new standards or policies Northrop Grumman is to view and accept the changes in order to assess if any costs will need to be implemented with the changes. John went on to explain that he is currently working on making SEC501 mirror NIST for more consistency across the COV. His goal is to publish the updated SEC501 by January 2011 with compliance by July 2011. David questioned whether there would be a fiscal or workload impact on the agencies with the proposed changes. John answered that once 2 or 3 sections are converted he would better be able to answer the question. Goran added that changing SEC501 will help in the mapping to the Federal 853, which is more of an industry standard.

David asked if there had been any recent security breaches and if any information could be shared about them. John said there had been no recent security breaches other than the ongoing email phishing.

David brought up his concern that agencies are in violation of SEC501 in regards to devices with persistent storage and that those devices might be removed from the agency premises while potentially storing images of sensitive data. John explained he is working with DGS on changing the Master Contract concerning the devices and the language will include options to Sanitize the device, Contract updates or Agency Purchase the Hard Drive. John added that a Leadership Communiqué was sent to Agency heads on August 11, 2011 concerning this topic. John noted that the Partnership is required to sanitize the devices, however no agency has returned a device to be sanitized as of yet. David asked what vendors fall under the contracts. John said he will get the names of the vendors and will forward the Leadership Communiqué to Council members.