



## Commonwealth Information Security Council Risk Management Committee Meeting

March 15, 2010  
2:00-3:00 pm CESC

### **Risk Management Committee members attending:**

Goran Gustavsson, Co-Chair  
Ed Miller, Co-Chair  
Ross McDonald, DSS  
Joshua Cole, Dept of Aviation

### **Risk Management Committee members absent:**

Bob Auton, DJJ  
Aaron Mathes, OAG, Co-Chair  
Jack Spooner, DOA  
Jeremy Greenwood, TRS

### **Topic: Risk Management – Updated direction for Committee**

- At the Security Council meeting (3/15/10), John Green had asked that the Risk Management Committee take a close look at the new VITA transformation legislation. In particular, we will be looking at the area of risk management from a Commonwealth perspective. Considering the changes (and new laws) surrounding the CIO's (i.e., VITA delegated) responsibilities regarding Information Security Risk Management.
- Before rewriting the deliverables, the consensus was that we should all become very familiar with the new legislation and the responsibilities it carries. The particular paragraph of interest follows in *italics*.

*H. The CIO shall also develop policies, procedures, and standards that shall address the creation and operation of a risk management program designed to identify information technology security gaps and develop plans to mitigate the gaps. All agencies in the Commonwealth shall cooperate with the CIO. Such cooperation includes, but is not limited to, (i) providing the CIO with information required to create and implement a Commonwealth risk management program; (ii) creating an agency risk management program; and (iii) complying with all other risk management activities.*

- For our meeting next month, we are hoping that everyone can come prepared with their interpretation of the new law so that the group can come to a consensus before we go in and re-think our deliverables for 2010.
- The Committee will consider developing guidelines for agencies and VITA to use when determining what data is needed by VITA.
- There was additional discussion about Risk Assessment metrics (to be determined) and supporting software that could be used.