

## **Comments on the Mainframe Computing Environments Security Assessment Guide from the Dept of Education:**

- What future activities does the Department envision using this guide? Self-assessments, IG Audits, etc? Some of the other documents already being used for other assessments might overlap some of the questions contained in this document, so before it is issued to the Dept, it should be vetted for those overlaps.
- This document is not completely sanitized yet and needs all the references to the old agency removed. There are still a number of references left. Also, the Dept would want to replace the old references with the appropriate ED references.
- Their instructions say that any “No” answers have to have the remediation actions listed on that form. At ED, usually the remediation plans and actions come after the assessment is completed. They have a comments section and action plan at the end of each section. I would suggest that the column for expected results be removed, because it is unnecessary, most SSOs have an idea of what the expected outcomes should be and instead replace it with a column at the end for comments. This way comments for each item can be listed.
- There should be a separate document with action items to fix the problems. This document only has a part at the end of each section for action items. This does not give enough space to adequately discuss the remedial actions for all the items in the section. It also does not call for a person to be assigned responsibility for the remedial action item, something that is vital to the item being successfully completed.
- The document should have a column for the question; maybe a column for expected results, a column for the result and a column for comments. The current column layout is extraneous and cumbersome.
- There isn't a clear mapping of where this requirement originated from, which is not good for Education purposes. Another Department used this document; logically there are questions in this document that were generated specifically for the other Department. However, there is no mapping to indicate if the questions came from NIST, OMB, or the other Department. The Department of Education should not be testing their mainframes with questions based upon other Department's requirements. It looks like a lot of the questions must have come from the other Department's requirements, because from experience with the Federal references listed, the questions do not originate from there.
- Again, it is hard to determine the appropriateness of the content because it seems like some of the references to the OS/application controls/etc are references to the other Department. Education has to only leave in what is applicable to this Department and that would make it easier for others to evaluate.