

Security Policy Comparative Analysis

Task Overview

During the last Task Order (TO 59.1), FSA asked KPMG Consulting to develop a set of policy statements drawn from the draft Department of Education policy document, NIST 800-18 (Guide for Developing Security Plans), ISO 17799 (Information Technology Code of Practice), and NIST 800-26 (NIST Self Assessment Guide). Because the Department was about to release its policy document as a final version, we were asked to do a comparative analysis between the two documents to detail what discrepancies existed between the two sets of guidance. These results were forwarded to the Department's CIO office, and will be incorporated into their next draft policy document.

Task Description

Because the initial creation of the FSA policy statements was partially based upon the Department's policy document, there was no need to determine what Education policies were missing from the FSA list. Therefore, our analysis focused solely on what policies were either missing or different in the Department's policy document, using the FSA list of statements as the control.

With the approach defined, we proceeded to search the Education policy document for each FSA policy statement to determine if the policies were consistent, partially consistent but containing gaps, or non-existent in the Education document. The findings of this analysis were presented in a table listing all the FSA policy statements, their corresponding Education policy (if available), and a color-coded description of what inconsistencies existed between the two documents. Further, following the FSA policy statement format, the analysis is divided into the policies areas of control: Enterprise Management, System Operational, and System Technical controls.

Upon completion of the analysis, an executive summary of major discrepancies was created detailing the more alarming or glaring inconsistencies between the two documents. This could be used as information during the Departmental CSO meetings, or a basic summary of the findings to present to the Departmental policy document owners. Some basic statistics that were discovered:

- 40/93 policy statements missing or incomplete in Departmental management controls
- 106/140 policy statements missing or incomplete in Departmental operational controls
- 90/124 policy statements missing or incomplete in Departmental technical controls

Task Status

Andy Boots forwarded our findings to the Departmental CIO office with the comment that the FSA policy compilation provides a "more complete policy/topic coverage than the current ED draft". Education's response was that they would forward the analysis to the Education team working on the improved version of the Department's policy document, and appreciated the input. The KPMG Consulting team currently is drafting an FSA Information Security Policy document, using the results of this analysis.