

GISRA Assistance

Task Overview

On July 1st, the Department of Education tasked its Principal Offices to complete several tasks by July 29th in support of the Department's GISRA submissions, including (for each system) the NIST Self Assessment questionnaire, a Critical Infrastructure Plan (CIP) questionnaire, system inventory worksheets, and remediation plans for the recently completed risk assessments. FSA asked KPMG Consulting to assist SSO's complete the forms, and then support the compilation and review of the completed submissions. As additional assistance, we created a prepopulated Self Assessment form containing answers regarding FSA policy and some procedures, assuring a uniform standard for FSA systems.

Task Description

Our first step was to prepopulate the NIST Self Assessment questionnaire. The questionnaire consists of 261 questions covering a variety of security controls. For each question, the respondent must answer whether the system has policy regarding the matter, has created procedures detailing how to enact the policy, whether those procedures have been implemented, whether they were then tested, and lastly if that aspect of security has been integrated throughout the agency. The method of grading the self assessments this year meant that credit would only be given for the most basic level of security at the system, i.e. a question would not get credit for implementation if there were no policy or procedures. In order to ensure consistency as well as a higher score for the PO, we examined the newly released FSA Information Security and Privacy document to determine where FSA could take credit for having policy. We provided a template version of our findings (complete with detailed remarks identifying where in the policy document one could find the applicable policy) to the SSOs so that they could concentrate on whether their systems had the procedures, and whether they had implemented and tested the same.

During the course of the next month, we worked with numerous SSOs to answer questions, provide clarifications, and otherwise make sure there would be no issue with meeting the July 29th deadline. The CIP effort entailed providing a rated response (with justifications for high rated items) for 83 questions regarding the system's importance to various Departmental goals. Inventory forms were required for all new systems or systems updating their sensitivity or criticality. The remediation plans actually had two parts: the first a chart including the planned method of correction, estimated completion date, and estimated cost; and the second a non-concurrence chart explaining why they disagreed with the risk assessment finding. The Security and Privacy team asked the SSOs to submit all GISRA materials on July 22nd to the team for review. During that last week, we looked through the submissions looking for inconsistencies and inaccuracies before we bundled them for submission to the Department.

Due to the sheer volume of material, we split up the reviews with one person in charge of reviewing one particular type of report as they came in. This yielded more consistent reviews, and sped up the process as we learned what areas tended to contain more problems. Feedback was provided via e-mails to the SSOs for their concurrence and resubmittal.

Task Status

All reports were submitted to the Department on time on July 29th.