

GISRA and NIST Self-Assessments

Task Overview

The requirement to complete the NIST Self-Assessments for SFA systems came to the SFA security office in June 2001. KPMG Consulting responded to this requirement by assisting the security office organize and structure its reply to OMB. The effort included a kickoff meeting with SFA SSOs, individual working sessions with SSOs, and compiling the responses for eventual submission to OMB. The process proved to be a successful venture for the security office, making SFA the only agency in the Department to comply with the July 18, 2001 deadline.

Task Details

KPMG Consulting's GISRA and NIST Self-Assessment support began in June with the initial briefing to SFA System Security Officer's. The briefing provided the SSOs and the security office with an initial overview of GISRA, the act's requirements, and a more detailed review of the Self-Assessment itself. The Self-Assessment contains sometimes confusing language that confused the SSOs and needed immediate clarification. For example, we explained how security is a process that progresses through various phases called policy, procedures, implementation, testing and integration. By clearly differentiating between each phase in the security cycle, the SSOs gained a deeper understanding of not only the assessment, but also security in general.

The briefing concluded with an invitation to each SSO welcoming them to sign up for individual work sessions with the security office and KPMG Consulting representatives. The majority of the SSOs leaped at the chance to meet with us one on one. We conducted ten to fifteen working sessions of three hours each over the course of one week to complete the Self-Assessments. The sessions varied from brief informational discussions to detailed, question-by-question analyses of the questionnaire. Throughout the process, both the security office and KPMG Consulting obtained a thorough understanding of the assessment, its imperfections, and solutions to many of the SSOs pressing concerns.

The final project to complete for the GISRA task area was to assist with SFA's submission to SFA and eventually to OMB. This task involved the consolidation of SFA's SSO responses to the Self-Assessment into the framework provided by the OIG. We assisted the security office prepare the document and present the findings to the Deputy CIO.

During the second portion of the task order, we assisted the security office respond to the corrective action plans that the Department of Education delivered to the SFA Security Office. The CAPs were a combination of several correction action plans the Department and SFA maintain. We responded to the request by pouring through the CAP item by item, determined the status of each weakness, and delivered our evaluation to the Department. The effort was successful, despite the convoluted corrective action plan provided by the Department.

Task Status

We completed SFA's GISRA CAP response on schedule. SFA will need to respond to GISRA again next year, and perhaps for the out years as well.