

## **Task 3.2 GISRA/FISMA Reporting**

### **Task Overview**

FSA, as part of the Department Of Education, must submit GISRA/FISMA\* reports annually to OMB. This process requires the completion of Self-Assessments and the creation of an agency-level report. To support this initiative, BearingPoint will create and conduct specialized Self-Assessment training courses for FSA employees and their contractor counterparts. Additionally, we will coordinate the submission of the Self-Assessments to the Department and implement a tracking program to measure performance against FSA's 2002 baseline.

Soon after the annual reports are submitted, OMB requires the creation of Plans of Actions and Milestones (POA&Ms) to document and track the remediation of weaknesses described in the annual report. With the POA&Ms established OMB requires quarterly reports (submitted by the Department) on the progress of all POA&M actions. To support this initiative we will work with the OCIO to track FSA POA&M actions, meet and work with the SSO's, system managers, and the contractors for FSA systems to make sure their actions are completed on time and recorded properly.

\*Due to the lack of FISMA implementation guidance, the ideas contained in this overview are based on the assumption that FISMA parallels much of GISRA and will be implemented in much the same manner.

### **Task Details Period 1**

We began supporting FSA's Security and Privacy team in January 2003, after the completion and submission of their 2002 annual report and POA&M actions.

The first steps in support of the security and privacy team was to assist FSA SSO's with updating and validating their Inventory Worksheet and CIP Survey. This was done for all FSA MA's, GSS's, and Applications. Once the SSO's reviewed, verified, and updated the information on the worksheet and Survey, we reviewed the information and submitted the updated FSA inventory (all GSS's and MA's) for review and submission to the Department (a biannual requirement). The information from the survey and worksheet also determined the Tier of the system (based on mission criticality, confidentiality, integrity, and availability of the system). We updated the FSA System Tier Identification Sheet also.

Our next area of support was the tracking and monitoring of POA&M action items that will be reported by OCIO to OMB in the quarterly report due April 1, 2003. We attended weekly meetings with OCIO to ensure consistency between our status information OCIO's. This included information on FSA items that were closed, still open, and late. This review is accomplished on a weekly basis (2-3 times a week) by checking the public folders for each tier 3 and 4 system and checking their POA&M sheets to see their status.

Since quite a few action items were late we decided to meet with each system on an individual basis to discuss in detail their status. Members of the Security and Privacy team, SMs, SSOs and contractors (as necessary) attended the meetings.

At the meetings we also distributed checklists for the systems to review their Disaster Recovery/Continuity of Support Plan and their Change Management Plan. We also requested (because of a new Department requirement) that for each action item that was late (or would be late by February 28, 2003) that they create steps and dates that would lead to the completion of the outstanding actions.

## **Task Details Period 2**

Period 2 of our task order began by working with the FSA systems that still had overdue (past the February 28, 2003 deadline) action items on their POA&Ms. We provided them a template to fill in information about the steps they would take to get the actions closed and the dates they expected to complete them. We then gathered their explanations and submitted them to ED/OCIO for review. We worked with the Department to make sure the actions we were reporting were consistent with those they still considered overdue. We continued to provide the Department with updates throughout March and had them remove any systems from the overdue list that had completed their actions before the April quarterly report was submitted to OMB. Due to the efforts of the Security and Privacy Team we were able to remove all but eight items from the overdue list.

We continued tracking and monitoring POA&M action items that will be due on May 5, 2003 as required by the Department and that will be reported by OCIO to OMB in the quarterly report due August 2003. We attended meetings with OCIO to ensure consistency between our status information and OCIO's. This included information on FSA items that were closed, still open, and still late. We contacted and reminded the SSO's of all the actions they have yet to complete that will be considered late after May 5. We continue to review their progress on a weekly basis (2-3 times a week) by checking the public folders for each tier 3 and 4 system and checking their POA&M sheets to see their status.

In another area of the task and in preparation for helping FSA systems fill out and complete their 2003 Self-Assessments for FISMA, we created an informational PowerPoint briefing that we provided to all the attendees of the April 1, 2003 SSO Security Training Meeting.

The briefing explained at a high level, that FISMA replaced GISRA and that there are some noticeable differences between the two acts. We notified them that the Self-Assessments would more-than-likely still be required and that they will need to complete them by May 30, 2003. This date is tentative due to the fact that OMB still has not released guidance as to how to comply with FISMA. It is expected that OMB will release this guidance at the beginning of May. We will then provide training to the SSO's and their contractor personnel. We also notified them in the briefing that FSA will begin to

track their level status on the Self-Assessments from year to year and expects to see progress.

**Task Status**

This task is ongoing. Currently, we are working with the systems to complete all POA&M actions due by May 5, 2003. These actions include the completion of Risk Assessment items, System Security Plans, and Contingency Plans. We also continue to work with OCIO to close any completed actions.

We stand ready to support the FSA FISMA effort to include training as soon as OMB releases guidance on the new law. The 2003 Self-Assessment process will begin shortly afterward and we will organize our team to support FSA's efforts.