

**US Department of Education
Student Financial Assistance (SFA)
Modernization Partner Program
Security and Privacy Infrastructure
Task Order 18 Monthly Report 8/30/00**

Overview

The office of Student Financial Assistance has made a significant investment in the Modernization Blueprint as the foundation of future process and systems improvements. These processes and systems should be implemented in a secure environment and in a manner that protects the personal, private information of students, parents, and borrowers. This task order proposes development of the security and privacy organization and processes necessary to support such a secure and private environment.

Overall Objectives

The objectives of this proposal are (1) to help SFA secure its current environment and (2) to plan its security and privacy strategy for new initiatives. The task order has the following four outcomes:

- SFA capability to perform risk and vulnerability assessments to identify and document security and privacy risks, recommend mitigating controls and assume business unit responsibility for residual risks as part of its ongoing security and privacy strategy
- A security and privacy organization to support the requirements of current and future business initiatives
- Policies & procedures syndicated with SFA business units and systems administrators
- Communication and training plan coordinated with SFA University and the Director of Communications to ensure that key security and privacy messages are communicated to SFA employees and business partners

Monthly Task Activities

During the period of August 10, 2000 through August 30, the SFA Security and Privacy Champion finished development of a training curriculum for System Security Officers (SSO), Security and Privacy Advocates, and System Managers within SFA. In addition, a plan to communicate security awareness and guidance throughout SFA was developed and shared with workshop invitees. The SFA Security and Privacy Champion plans to regularly schedule training in order to enhance security awareness and provide more specific role-based training.

Risk assessment work was completed on time due to the intervention of the Security and Privacy Champion. Some system specific detailed information was slow in delivery due to workload constraints on the part of the System Managers. The Risk Assessment report provides a basis for the System Managers and SSO's to develop major application security plans targeted for completion Oct 1, 2000.

The A-130 report for the SFA managed systems was combined into one deliverable report with system specific detail and recommendations. This consolidated report follows the logical structure of the Meridan Virtual Data Center, which has located most information processing infrastructure in one physical facility. In the future, A-130 reviews can now be conducted on a tri-annual basis for all systems, and this single effort should result in cost savings to the government.

Major Task Activities Planned Through August 30, 2000

- Deliver the draft A-130 reviews of SFA major applications;
- Conduct two Security and Privacy Workshops for SSOs;
- Develop a Security and Privacy Awareness day agenda; and
- Participate in meetings on security standards and policy.

Major Task Activities Completed Through August 30, 2000

- Delivered the draft A-130 reviews of SFA major applications;
- Planned to conduct two Security and Privacy Workshops for SSOs scheduled in September;
- Developed a Security and Privacy Awareness day agenda; and
- Participated in meetings on security standards and policy.