

**US Department of Education
Student Financial Assistance (SFA)
Modernization Partner Program
Security and Privacy Infrastructure
Task Order 18 Monthly Report 6/14/00**

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

The Security team is developing documentation and training materials on SFA security and privacy policies and procedures (based on Department of Education/Government-wide policies). The team delivered a draft report to the SFA Security and Privacy Champion, Andy Boots, on 6/11/00. This is currently in a review and edit process with Mr. Boots. It is anticipated that this will be completed and available for comment within SFA by July.

The security team reviewed existing risk assessment reports and created a table of attributes for use in a tracking database. This critical evaluation will assist in conducting the application risk reviews this summer, and aid Mr. Boots and his staff to evaluate risk management and mitigation progress of the system managers and security officers. An analysis of the risk assessments revealed a number of common concerns and laid the basis for tracking attributes. A copy of this evaluation is attached to this deliverable report.

The risk assessment team met with Department of Education Security Management and developed an approach to the risk assessments to be completed by August 18, 2000. This completion date will be successful if the functional system managers buy into the process and rapidly provide source matter experts to this task. There is risk in this area if some managers are overly burdened and do not complete the requested action items, or meet with security team personnel, which is critical prior to beginning individual application risk assessments. Mr. Boots has tried to jumpstart the process by notifying the functional managers of the upcoming risk assessments and identifying early willing candidate system managers.

The security team developed a communication plan outline, and a draft was delivered to Mr. Boots for comment. His comments were incorporated and work on the communications plan will begin the week of June 19. This will be the basis for a framework of security program thinking and outline the tasks that are necessary to achieve the vision of an improved security and privacy program for SFA.

Major Task Activities Planned Through July 10, 2000

- Complete a Communications Plan
- Complete Security/Privacy Guidance, based on feedback from CIO review; circulate to security and system contacts in the Channels for review and buy-in;
- Participate in monthly Departmental and security related meetings;
- Begin A-130 security reviews (LO/LC, Pell/RFMS, VDC, and school visits);
- Begin to develop a training program for SFA security personnel;
- Develop requirements for an incident/corrective action tracking system;
- Discuss with acquisitions personnel how to incorporate security features and clearance penalties into performance-based contracts; and
- Begin planning for a SFA Security Awareness Day