



Business Case

Project Name: Security Policy Administration and Execution

Channel: OCIO

Project Sponsor: Wayne Wright

Project Lead: Andy Boots

Project Description

Describe the need for change (the business problem to be addressed).

As part of its commitment to customers and partners, SFA manages risks on a continuous basis. More and more, SFA needs to demonstrate that its risk management practices are consistent with best security practices and U.S. Public Law and policy. Security incidents could undermine the credibility of SFA, and greatly affect its ability to help put America through school. In addition to losing face, actual fraud and abuse could occur without adequate security and privacy controls. The result of this task should be comprehensive life cycle security policy, controls, risk assessment, measurement, incident response, basic security understanding, research, and training across SFA.

What is the purpose of the initiative?

The purpose of this initiative is to strengthen security and privacy in SFA with both short term fixes and continuous activities.

Short Term:

- 1) Develop a technical approach and architecture to Single Sign-on for the School Web Portal.
- 2) Publish security procedures and policy on the SFA intranet site.
- 3) Develop and publish templates and SDLC security checklists for compliance with public law.
- 4) Develop service level agreements for logging, intrusion detection and incident response.

Continuous:

- 5) Mentor and train SFA employees to follow good security practices.
- 6) Track and respond to external requests for evidence of compliance with public law from the Department of Education Information Security Office and IG, OMB and GAO. (GISRA)
- 7) Respond to requests for security guidance and plan for incident response.
- 8) Provide technical security experts to SFA to perform research and security architecture planning.

The result will be a strong security and privacy program that will increase customer and employee satisfaction by making sure controls are in place to make the systems more available, reduce the potential for data theft and improve protection of privacy information. The measurement of success will be the effectiveness in these critical protection areas:

- a. Prevent data theft from SFA (*integrity*);
- b. Prevent unauthorized viewing or alteration of other people's data (*confidentiality*);
- c. Prevent service disruption (*availability*); and
- d. Provide for clean security audits (*auditability*).



What is the scope of the initiative, including what it is not?

This initiative provides professional support to complete required tasks. It does not provide software or hardware. This initiative includes development of architecture, policy, procedures, checklists, and templates, but does not include risk assessments of individual systems or major applications. Independent risk assessments are funded by system owners as part of the solution development life-cycle.

This initiative will complete establishment of an operational security and privacy program in SFA and will:

- Gather requirements, create the solution design with costs for Single Sign-on for the School Web Portal for designated back-end systems to ensure appropriate access by authorized users with minimal difficulty;
- Document the School Portal SSO requirements from an enterprise perspective and in a format that can be used for an authentication gateway design project that may be funded in a subsequent business case; (this is not a throw away effort)
- Publish the security policy on the SFA Intranet and Extranet websites so employees and operating partners have access to up-to-date security guidance in one place, which increases their knowledge of what rules to follow that later will be audited for compliance;
- Develop templates, checklists, and materials for use by employees and contractors during the systems development lifecycle, including, but not limited to checklists for independent ("A-130") risk assessments and penetration tests to ensure secure systems and compliance with public law;
- Define the minimum requirements for system logging, intrusion detection, and incident response to prevent and detect data theft, alteration of data, viewing by unauthorized persons;
- Train SFA employees, contractors, and partners, including, but not limited to SFA System Security Officers and business units on security planning, incident response and continuity of operations;
- Research emerging and established security and privacy technology, including, but not limited to, assessment of outsourced security services which might be used by SFA and its partners; and
- Identify best security and privacy practices in government and industry and bring them to the attention of SFA management.

What is the start date and end date of the initiative?

The proposed start date of this project is May 1, 2001 and projected end date is September 30, 2001.

What other business areas/external groups are affected by the implementation of this initiative and how are they affected?

Security and privacy affects all SFA programs, systems, organizations, and partners. In particular, SFA systems and the systems of partner organizations will be able to operate within a known security and privacy risk environment, which should lead to increased customer confidence and better regard by audit and oversight organizations, including the Education Department Inspector General, OMB, GAO and the Congress.

What systems are impacted by the implementation of this initiative and how are they impacted?

This initiative will help SFA live up to its value of trustworthy system by making sure that system confidentiality, integrity, and availability are supported throughout the life cycle of each system. All SFA systems are covered by the policies in this program. Without proper attention to security, system



funding could be affected, and program funds could be reduced or removed due to ineffective security controls and management.



What business processes are impacted by the implementation of this initiative and how are they impacted?

Security permeates all SFA business processes and can affect them positively or negatively.

Technologies Used

No new technology will be used in this project.

Benefits

This effort will enhance security documentation which leads to better understanding by oversight officials. Confidence in the systems integrity could enhance use and business unit growth. Not performing adequate security management could result in millions of dollars in damages and loss. Adequate security will re-enforce use of electronic processes that are more cost effective than paper-based processes. It is well documented that security programs do not lend themselves well to quantitative metrics.

Costs

Provide costs, including those to implement the initiative and the costs to support it over its useful life.

COSTS						
	BY	BY+1	BY+2	BY+3	BY+4	Total
Development	<u>\$ 1,000,000</u>	<u>\$400,000</u>				
Operations						
Prod. Proc						
Key Pers.						
Ad Hoc						
Sys. Maint.						
Telecom.						
Data Center						
Sub. Ops						
Total						
<i>Assumptions</i>						



Total Cost of Ownership

What is the level of required enhancement after implementation?

Security is an ongoing process that will never go away. Additional personnel could be hired to augment the current staff, which would reduce contractor spending.

What is the life span of this initiative?

This project will correct deficiencies in planning for security incidents and response, but it should be noted that a significant portion of this work will continue from year to year as security is a continuous process.

Alternatives

Discuss what could be done in place in this initiative and describe the consequences of each alternative.

Alternative	Consequence
Remain as-is	Fragmented, uncoordinated SFA system security, lower customer trust, GAO audits, reduced OMB funding.
Enhance an existing system	Not applicable.
Implement on a smaller scale	Significant risks would remain without proper documentation.

Risks

Risk	Description of Risk	Mitigation Strategy
Financial	Project takes longer than expected, thus driving up labor costs	Make sure contractors have a clear scope and a well-defined project plan. Use a fixed-price bid format.
Technology	Technology provider goes out of business	Contractors will be using proven technology developed and provided by industry leaders.
Scope	Try to solve all security problems at once	Maintain focus on one task area at a time.
Management	Business stakeholders (channels) fail to buy into security improvements.	Implementation of the security policy must be understood as a strategic program, supporting all business units
Exposure	Security policy delivered too late	Coordination of time frames and schedules by SFA manager.

Acquisition Strategy

Sources (Indicate the prospective sources of supplies or services that can meet the need of this project. List the most likely offerors for the requirement, and/or the manufacturer and model of the equipment that will most likely be offered).

Modernization partner.



Competition (Describe how competition will be sought, promoted, and sustained throughout the course of the acquisition, including any performance requirements that will be required).

Already competed.

Contract Considerations (For each contract contemplated, discuss contract type selection; use of multiyear contracting, options, or other special contracting methods, ex: performance-based).

N/A

Schedule/Milestones (including acquisition cycle)

#	Milestone	Start Date	End Date
1	Task award and meeting with contractor task manager	5/1	5/7
2	School Portal Single Sign-on Design with implementation costs	5/28	8/31
3	Develop and publish Intranet Security Handbook	5/7	7/10
4	Create SDLC Checklists and PRR Checklists	6/4	8/31
5	Create Intranet and Extranet content updates - monthly	5/31, 6/28 7/26, 8/30	9/28
6	Create logging requirements and draft Service Level Agreements for security monitoring of IDS and server logs	6/1	8/31
7	Create template for independent risk assessments	7/2	7/31
8	Create incident response guidance for system managers and owners	8/1	9/28
9	Conduct Security Training on a monthly basis for System Security Officers	5/31, 6/28 7/26, 8/30	9/27
10	Review and monitor corrective action plans	5/1	9/28