

SFA Modernization Program
United States Department of Education
Student Financial Assistance



Single Sign-On
Requirements Definition - DRAFT

Task Order #82
Deliverable #82.1.2

DRAFT

February 15, 2001

Document Revision History

Version No.	Date	Author	Revisions Made
1.0	February 15, 2002	Michael Bruce	Initial draft released
1.1			Revised draft released
1.2			Final draft released

Table of Contents

EXECUTIVE SUMMARY	4
1 INTRODUCTION.....	6
BACKGROUND.....	6
PURPOSE	6
SCOPE	6
DOCUMENT REFERENCES.....	7
ORGANIZATION OF THIS DOCUMENT.....	7
2 TARGETED USERS	8
3 REQUIREMENTS.....	9
REQUIREMENTS TRACEABILITY MATRIX	10
1 Authentication and Identification.....	10
2 User Management.....	13
3 Session Management.....	19
4 Access Management.....	20
5 Customer Care.....	24
6 Legal.....	25
7 Environment.....	26
8 Operations.....	28
9 Audit and logging.....	29
10 Handling of Data	30
11 Performance and Scalability Requirements.....	31
12 Availability.....	33
13 Security Requirements.....	35
3 POTENTIAL ALTERNATIVES.....	42
CUSTOM DEVELOPED SINGLE SIGN-ON SERVICE.....	42
SINGLE SIGN-ON BY ENHANCED CURRENT SFA CAPABILITY	42
COTS ENABLED SINGLE SIGN-ON SERVICE.....	43
SINGLE SIGN-ON SERVICE FROM A MANAGED SERVICE PROVIDER	43
APPENDICES.....	45
APPENDIX A: IPT TEAM.....	46
APPENDIX B: ACRONYMS AND ABBREVIATIONS	47
APPENDIX C: SFA LOGIN/ACCESS SURVEY RESULTS AND SUMMARY.....	48

Executive Summary

This document identifies business and technical requirements for a Student Financial Assistance (SFA) Single Sign-On service, compiled and recommended by an enterprise IPT and IPT advisory team. These requirements were compiled as a result of interviews conducted within SFA, industry and market research, and past efforts related to Single Sign-On services.

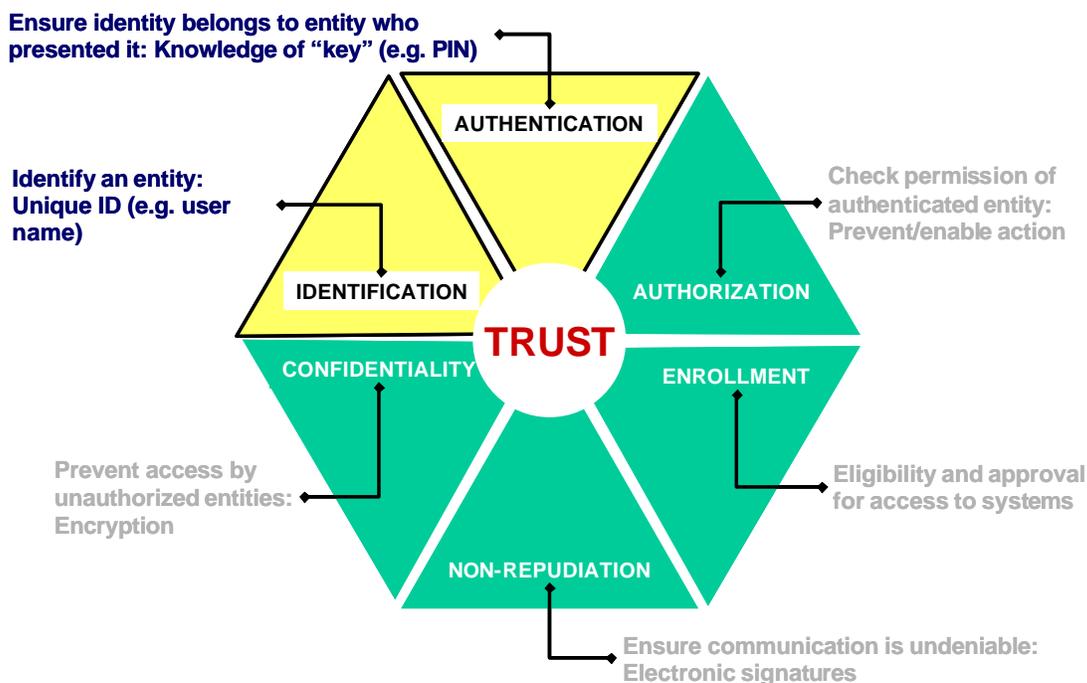
These requirements will serve as the basis for evaluating, selecting, designing, and tailoring the appropriate Single Sign-On service for SFA if funded and approved by the SFA IRB.

The business driver for a Single Sign-On service at SFA is the:

- Need to Simplify Customer Access to SFA Systems
 - SFA system users have multiple logins/IDs/passwords
 - Customers want single access to multiple SFA systems
 - Modernization & Integration efforts implementing additional logins

The objective of this effort is to: Identify single sign-on business & technical requirements. The objective of this effort is not to: Define the single sign-on solution during this phase

The scope of this effort is to identify requirements for Identification and Authentication. The scope does not include the areas of Authorization, Enrollment, Non-repudiation, and Confidentiality.



The effort has resulted in the following:

- Assessment of 45 current and future SFA systems for login and access needs

- Identification of 24 unique access credentials for SFA systems:
 1. COD Login
 2. Pell ID
 3. TG (TIVWAN) Number
 4. DLO Login ID
 5. DSLI Login ID
 6. DLSS Username
 7. DLCS Login ID
 8. SFA PIN Username - SSN, first 2 letters of last name, DOB
 9. EDNet User ID
 10. DMCS/FFEL Username
 11. OPEID
 12. TIN (Taxpayer Identification Number)
 13. ERM Username
 14. FMS Username
 15. GAPS UserID
 16. Jamcracker UserID
 17. IFAP Username
 18. IAM Username
 19. CPS UserID
 20. NSLDS UserID
 21. OCTS Username
 22. PEPS Username
 23. Citrix Username
 24. School Portal Username

1 Introduction

Background

As part of its commitment to customers and partners, SFA manages risk on a continuous basis. In view of this, SFA recognizes that there is a need to provide system access controls that enhance a user's online experience allowing for a closer relationship to SFA and greater reliance upon SFA services and applications. At the same time access services must adhere to SFA identification and authentication policies, and U.S. Public Law and policy.

Currently, system users may utilize multiple access credentials to logon to SFA systems, which may also have multiple and differing Channel-specific access points. Approximately 25,000 School and Financial Partner users access SFA systems on a regular basis as part of regular student financial aid processing and administration. Over 23 million students have on-line access to SFA systems in order to complete FAFSA submissions and conduct other student aid related business.

In addition, as new and reengineered systems are released, additional access credentials and rights may also be created. New applications will also increase use of SFA's electronic channel. This could create increasing opportunities for unauthenticated access to SFA systems, undermining the credibility of SFA, and affecting its ability to help put America through school. To reduce the risk inherent in multiple access points, a Single Sign-On service is being considered.

Purpose

The purpose of this task is to define the enterprise requirements for the development of a Single Sign-On service for SFA systems. The key objectives of this document are to:

- Capture and document the requirements that apply to the design, implementation, and operation of a Single Sign-On service for SFA system users and administrators,
- Provide guidance and evaluation criteria for the selection of a Single Sign-On service,

Scope

This document defines the requirements necessary to select, design, implement, and deploy a Single Sign-On service for SFA systems. The requirements were gathered by an enterprise IPT, and included past Single Sign-On studies, discussions with channel stakeholders, market research, and interviews with SFA staff. The IPT leveraged guidance from the Single Sign-On advisers throughout the process.

It is anticipated that an SFA Single Sign-On service can provide the following benefits:

- Improved customer access to SFA systems – [Common](#) Identifier
- Support the access needs for SFA's Portals and overall eCommerce strategies
- Strengthened cyber-security – [Trusted](#) Identifier

- Establish a [Reusable](#) Single Sign-On service for SFA systems
- Provide potential future economic [Savings](#):
 - System enrollment
 - User access management
 - Reduced customer support for login

The scope of this effort is to identify requirements for Identification and Authentication. The scope does not include the areas of Authorization, Enrollment, Non-repudiation, and Confidentiality.

Document References

The following documents were used in establishing the requirements for the Single Sign-On initiative:

- RFI for Single Sign-On Software, Department of Education, Student Financial Assistance, July 2001
- Single Sign-On Requirements Analysis for DLOS, June 14, 2001.
- OMB Circular A-130, Appendix III
- Common Criteria v2.1 (ISO: IS15408), September 2000
- NIST Special Publication 800-18, December 1998
- RFI response review, TO59, August 31 2001
- Statement of objectives – Single Sign-On Requirements and Design
- Business Case, Single Sign-On Requirements and Design

Organization of this Document

The following information outlines the organization of this document:

- **Executive Summary**
- **Section 1³/₄ Introduction** provides an overview of Single Sign-On task.
- **Section 2³/₄ Users** provides a list of the potential users of the Single Sign-On service.
- **Section 3³/₄ Requirements** provides the results. The requirements represent the business, functional and technology needs for an SFA Single Sign-On service.
- **Section 4³/₄ Potential Alternatives** provides an early observation of possible alternatives. The next phase of this task, if funded, will utilize the result of this analysis to analyze and recommend alternatives.
- **Appendix A – IPT List** lists the individuals involved in completing and reviewing the work effort documented in this deliverable.
- **Appendix B - Acronyms and Abbreviations** contains definitions for acronyms and abbreviations used in this documents and within the SFA environment.
- **Appendix C – SFA Login/Access Matrix** contains the results of the data collection and summarization across 45 SFA current and planned systems.

2 Targeted Users

The Single Sign-On service is directed to external as well as internal users and administrators. Upon deployment of Single Sign-On, these users will be able to multiple access systems from SFA portals with a single set of user identification/authentication credentials (e.g., User-id and Password). Additionally these users will be able service many basic support needs.

The following chart describes each of the users of the Single Sign-On service:

User	Role in Single Sign-On Process
Students	
Students	User of SFA systems
Parents	User of SFA systems
Schools	
School Financial Aid Staff	User of SFA systems
Bursar's Office	User of SFA systems
Registrar	User of SFA systems
Delivery Point Administrator	Designated School employee to administer school-only access to SFA systems for school staff
Financial Aid Partners	
Lenders and Services	User of SFA systems
Secondary Markets	User of SFA systems
Guaranty Agencies	User of SFA systems
Servicing Agency	User of SFA systems
Access Administrator	Designated Financial Partner employee to administer financial partner-only access to SFA systems for financial partner staff
SFA Staff and Contractors	
SFA System Security Officer	SFA Enterprise Administrator to provide access to a particular SFA system for all internal and external users
SFA System Manager	SFA Enterprise Administrator to manage overall operations, including access, to a particular SFA system for all internal and external users
Contractor/Operating Partner Support Staff	SFA Enterprise Administrator to take actions to add users to a particular SFA system for all internal and external users.

3 Requirements

The requirements are divided into various sections, each focusing on an area representing a homogeneous set of related requirements. All the requirements in this document are presented in a uniform notation, with the following standard table format:

Identifier		
Title		
Description		
Source		
Assumptions		
Sub-requirements		

The fields in the table have the following meaning:

- **Identifier:** a unique identifier for each requirement.
- **Title:** a short description of the requirement.
- **Description:** a detailed description of the requirement.
- **Source:** from which area the requirement has originated.
- **Assumptions:** any specific assumptions made for this requirement (business channels to which the requirement applies, noteworthy consequences of this requirement and dependency of this requirement on others not in the scope of this project for fulfilling the requirement in its entirety).
- **Sub-requirements:** id and short description of sub-requirements of the present requirement. Sub-requirements represent detailed implications or further refinements of the broader requirement. The identifier is in the form <requirement id>.<number>, where number starts from 1.

Requirements Traceability Matrix

The following presents the requirements for a Single Sign-On service to support SFA systems.

1 Authentication and Identification

Identifier	1.1	
Title	Support different username formats as required by SFA business units	
Description	Ability to implement different user name syntax rules, defined by SFA.	
Source	SFA Login/Access Survey	
Assumptions	This enables the Single Sign-On application to utilize current and future user name formats.	
Sub-requirements	1.1	Support a minimum username length of 7 character
	1.2	Support a maximum username length of 12 characters
	1.3	Support use of the SFA-PIN Username (i.e., SSN, Date of Birth, First two letter of last name)
	1.4	Support use of the EDNet Username
	1.5	Support syntax rules that allow the following elements to be incorporated into usernames: <ul style="list-style-type: none"> • First Name Initials • Last Name • Office Code • OPEID • SFA PIN Username • Defined numeric value • Two or more data elements

Identifier	1.2	
Title	Support different password formats as required by SFA business units	
Description	Ability to implement different password syntax rules, defined by SFA.	
Source	SFA Login/Access Survey	
Assumptions	This enables the Single Sign-On application to utilize current and future password formats.	
Sub-requirements	1.2.1	The service should include features to translate unlike User Login Information from different agent platforms.
	1.2.2	Support a minimum password length of 4 character
	1.2.3	Support a maximum password length of 10 characters
	1.2.4	Support use of the SFA-PIN “Password” (i.e., 4-digit number generated by the SFA-PIN service)
	1.2.5	Support use of free-format Passwords

	1.2.6	Support syntax rules that allow the following elements to be incorporated into passwords: <ul style="list-style-type: none"> • Alphanumeric values • Alpha-only values • Numeric-only values
	1.2.7	Support rules that enforce the following capabilities: <ul style="list-style-type: none"> • Password lifetime from 30 to 120 days • Unlimited password lifetime • Comparison to previous passwords for the user • Disabling of the account after a period of inactivity of 90 to 365 days
	1.2.8	Store passwords in an encrypted state in the credential repository

Identifier	1.3	
Title	Support ED password syntax rules and management rules	
Description	Ability to adhere to ED password policies	
Source	ED OIG	
Assumptions	Adherence to ED policy guidelines.	
Sub-requirements	1.3.1	Support a minimum password length of 8 characters
	1.3.2	Support syntax rules that enforce at least three of the following conditions on every password: <ul style="list-style-type: none"> • Uppercase alphabetic characters (A-Z) • Lowercase alphabetic characters (a-z) • Numeral values (0-9) • Non-alphabetic and non-numeric characters (< ! @ # etc.)
	1.3.3	Support rules that enforce the following capabilities: <ul style="list-style-type: none"> • Password expires on the first logon attempt for a new user • Current user passwords expire and must be reset after 90 days • Password uniqueness set to 12 - i.e., systems stores and recalls past 12 passwords • Automatic account lockout after 3 unsuccessful login attempts • Set Account Lockout button • Automatic lockout duration set to 30 minutes • Unsuccessful login counter reset to 0 from 3 after 30 minutes

Identifier	1.4
Title	View own access rights
Description	The infrastructure should make it possible to display to an end user the applications or portals to which he/she has access.
Source	Best Practice
Assumptions	None

Identifier	1.5	
Title	Centralized user authentication	
Description	Centralize user authentication across all integrated applications, services, and other capabilities.	
Source	Best Practice	
Assumptions	Portals and applications must be capable of delegating user authentication to the Single Sign-On infrastructure, either explicitly or by allowing for logon emulation.	
Sub-requirements	1.5.1	Communicate to the applications and portals at run-time the identity of the authenticated user, and profile information associated to that user.
	1.5.2	For those portals or applications that cannot delegate user authentication, the infrastructure must be capable of performing an emulation of the end user logon in a way that is transparent to the end user.

Identifier	1.6 (Technical)	
Title	Authentication	
Description	The authentication mechanism must be configurable and extensible.	
Source	Best Practice	
Assumptions	None	
Sub-requirements	1.6.1	Provide a standard's based API (Plug-able Authentication Modules - PAM) to allow for additional authentication mechanism.
	1.6.2	Provide Username/Password authentication module.
	1.6.3	Provide Username/PIN authentication module.
	1.6.4	Based on the risk, different groups may utilize stronger authentication.

2 User Management

Identifier	2.1	
Title	Access rules administration	
Description	Provide a mechanism for a privileged administrator to change access rights of individuals or groups. Changes must be effective immediately, with quasi real-time effectiveness.	
Source	SFA Login/Access Survey	
Assumptions	None	
Sub-requirements	2.1.1	Administrator changes will be logged and audited
	2.1.2	Logon required to access user and authentication data.
	2.1.3	Provide capabilities to administer – <ul style="list-style-type: none"> • Passwords • User names • Recorded user data • Session management
	2.1.4	Provide a display for administrators to view access rights and privileges of all users.
	2.1.5	Real-time user status monitoring and user management.
	2.1.6	Allow custom access rules designed based on application specified attributes.
	2.1.7	Allow access control rules to include configurable conditions based on data from multiple data sources.

Identifier	2.2	
Title	Delegated administration	
Description	Allow for delegated administration of access policies and functions for an application or a set of applications to appointed administrators granted limited administration and management rights.	
Source	Best Practice	
Assumptions	None	
Sub-requirements	2.2.1	A privileged administration interface must be widely accessible from the SFA Intranet or the internet.
	2.2.2	Provide a graphical interface for administrators.
	2.2.3	Provide remote access capabilities for administrators.
	2.2.4	Provide integration capabilities to Call Center technologies via APIs, web-link, or other mechanisms.
	2.2.5	Provide an administration interface for administrators.
	2.2.6	Provide for integration of existing user management services.

Identifier	2.3	
Title	Ability to Group Users	
Description	The service should enable the grouping or categorization of like users where able. These groups should be handled the same way individual users are handled.	
Source	Best Practices	
Assumptions	This will enable more efficient administration of access authority.	
Sub-requirements	None	

Identifier	2.4	
Title	User Credential Store Integration	
Description	Provide the capability to communicate user credentials to existing SFA user credential repositories	
Source	SFA Login/Access Survey	
Assumptions	None	
Sub-requirements	2.4.1	ODBC Database (Oracle, SQL Server, Informix)
	2.4.2	RACF
	2.4.3	NT Network
	2.4.4	SFA PIN Service
	2.4.5	Directory (LDAP)
	2.4.6	Oracle Financials ERP

Identifier	2.5	
Title	Username and Password Generation	
Description	Provide the capability to create usernames and passwords or accept usernames and passwords created by trusted sources.	
Source	SFA Login/Access Survey	
Assumptions	None	
Sub-requirements	2.5.1	Automatically generate usernames adhering to SFA or ED username syntax rule
	2.5.2	Allow users or system administrators to manually create user names adhering to SFA or ED username syntax rule
	2.5.3	Automatically generate passwords adhering to SFA or ED password syntax rule
	2.5.4	Allow for the use of the SFA PIN – user name

	2.5.5	Allow for the use of the SFA PIN as the authentication credential
	2.5.6	Force new users to change the password upon initial logout; except when the SFA PIN is used to authenticate a user.

Identifier	2.6	
Title	User data normalization elements	
Description	Sub-requirements may vary may systems to identify users across applications	
Source	SFA Login/Access Survey	
Assumptions		
Sub-requirements	2.6.1	First Name
	2.6.2	Last Name
	2.6.3	Last four digits of the users social security number
	2.6.4	Telephone contact number

Identifier	2.7 (Technical)	
Title	User setup	
Description	The Single Sign-On solution must allow for flexible creation of usernames.	
Source	Best Practice	
Assumptions	None	
Sub-requirements	2.7.1	User data is captured electronically
	2.7.2	Username creation is automated.
	2.7.3	Username creation is based on definable rules.
	2.7.4	Initial password generation is automated.
	2.7.5	Initial password generation is based on definable rules.
	2.7.6	Initial password is communicated securely to the user.
	2.7.7	User is forced to change initial password at the first time.
	2.7.8	A batch registration of users must be offered.

Identifier	2.8 (Technical)	
Title	User removal	
Description	The Single Sign-On solution must allow for immediate and automatic removal of users.	
Source	Best Practice	
Assumptions	None	
Sub-requirements	2.8.1	A Single Sign-On administrator must be able to revoke Single Sign-On access for a user to any SFA systems within the administrator's domain.
	2.8.2	The process of removing a user must be automatic, once invoked by the administrator.

Identifier	2.9 (Technical)	
Title	Temporary disable user accounts	
Description	The Single Sign-On solution must allow for the option to disable accounts based on inactivity, definable number of unsuccessful login attempts.	
Source	Best Practice	
Assumptions	None	
Sub-requirements	2.9.1	If a user does not login for a specific time, users account is disabled. The timeframe must be configurable.
	2.9.2	If an account encounters multiple failed login attempts, it must be disabled after a configurable number of failed attempts.
	2.9.4	The Single Sign-On must allow disabling a user account for an unlimited timeframe.

Identifier	2.10 (Technical)	
Title	Password administration	
Description	Password administration must be automated and only require minimal manual interaction with the Single Sign-On administrator.	
Source	Best Practice	
Assumptions		
Sub-requirements	2.10.1	Users who have forgotten their password must request a new password by answering one or more free definable security questions.
	2.10.2	Users wanting to change their password must do this by providing their old password and answering one or more free definable security question.
	2.10.3	User is limited to a configurable number of password changes per day.
	2.10.4	A user must get a confirmation of a password change.
	2.10.5	Security questions must be configurable to rotate.
	2.10.6	Security questions are based upon data stored in the Single Sign-On user data store.

Identifier	2.11 (Technical)	
Title	User credentials creation	
Description	User credentials are subject to definable quality standards.	
Source	Best Practices	
Sub-requirement	2.11.1	Provide the ability to check for weak credentials based on definable syntax rules (i.e. Minimum password length, combination of number and letters, etc.).
	2.11.2	Provide the ability to check for weak credentials based on dictionaries.
	2.11.2	User credentials must have a definable lifetime. A warning message must be provided at a definable time before a credential is going to expire.
	2.11.3	A definable number of credentials used before must be stored. (e.g. Do not allow repeating passwords)

Identifier	2.12 (Technical)	
Title	User credential storage	
Description	User credentials must be stored securely	
Source	Best Practices	
Assumptions	None	
Sub-requirements	2.12.1	Credentials must be stored with one-way encryption in place (i.e. salted Hash).
	2.12.2	Storage of user credentials must allow for easy data synchronization/replication between SFA systems and the Single Sign-On data store.

3 Session Management

Identifier	3.1
Title	Integrated session management
Description	The infrastructure must be able to establish a session with the end user, allowing him/her to connect seamlessly across multiple sites with the initial successful login and authentication. The session should be logically shared across all the integrated portals and applications.
Source	Best Practice
Assumptions	Some applications (typically custom-built) may be able to directly use the session management services provided by the Single Sign-On infrastructure for their session tracking purposes. Other applications will establish their own sessions with the end-user.

Identifier	3.2 (Technical)	
Title	Session Timeout	
Description	The Single Sign-On mechanism must offer session management	
Source	Best Practices	
Assumptions	None	
Sub-requirement	3.2.1	The Single Sign-On solution must provide the option to prevent concurrent sessions for a user.
	3.2.2	The Single Sign-On mechanism must provide a configurable session timeout.
	3.2.3	A logout button must be available at any time.

4 Access Management

Identifier	4.1	
Title	Support User Exit/Signoff functions	
Description	Support exit/signoff options to end a user's active session with all applications accessed through Single Sign-On.	
Source	SFA Login/Access Survey	
Assumption	This provides the capability to end user sessions upon culmination of user activity	
Sub-requirements	4.1.1	Provide the ability for the Single Sign-On service to end an active user session after a predetermined period of user inactivity (i.e., timeout period)
	4.1.2	Provide the ability to end Internet session upon termination of a browser instance.
	4.1.3	Provide a logout button for users to a session directly

Identifier	4.2	
Title	Removal of users from Single Sign-On access	
Description	Support the removal of users from the Single Sign-On service	
Source	SFA Login/Access Survey	
Assumption	None	
Sub-requirements	4.2.1	Remove users from the Single Sign-On service within one business day after receiving notification by SFA
	4.2.2	Provide the ability to manually remove a user from the Single Sign-On service
	4.2.3	Provide the ability to automatically remove a user(s) from the Single Sign-On service

Identifier	4.3	
Title	Access administration	
Description	Provide tools to administer access to applications and resources	
Source	SFA Login/Access Survey	
Assumption	None	
Sub-requirements	4.3.1	Provide user self-service administration/help
	4.3.2	Allow users to maintain multiple sessions with applications. Applications will determine whether single or multiple sessions are allowed.

Identifier	4.4	
Title	System access mechanisms	
Description	Provide access to applications by various mechanisms	
Source	SFA Login/Access Survey	
Assumption	Browser-based sessions are the preferred means to connect to applications	
Sub-requirements	4.4.1	Provide access to application via the Internet

Identifier	4.5	
Title	User Authentication	
Description	Users are individually authenticated via passwords, tokens, or other devices	
Source	NIST SP 800-18	
Assumption	None	
Sub-requirements	4.5.1	Maintain and approve a current list of authorized users and their access.
	4.5.2	Digital signatures, if used, conform to FIPS 186-2.
	4.5.3	Access scripts with embedded passwords are prohibited.
	4.5.4	Emergency and temporary access can be authorized.
	4.5.5	Terminated, transferred, or otherwise ineligible individuals are removed from system access.
	4.5.6	Passwords are changed at least every ninety days or earlier.
	4.5.7	Passwords are unique and difficult to guess (e.g., passwords require alpha numeric, upper/lower case, and special characters)
	4.5.8	Inactive user identifications are disabled after a specified period of time.
	4.5.9	Passwords are not displayed when entered.
	4.5.10	Procedure exists to terminate lost and compromised passwords.
	4.5.11	Passwords are distributed securely and users are informed not to reveal their passwords to anyone (social engineering).
	4.5.12	Passwords are transmitted and stored using secure protocols/algorithms.
	4.5.13	Vendor-supplied passwords are replaced immediately.
	4.5.14	A limited number of invalid access attempts are allowed for a given user.

Identifier	4.6	
Title	Logical Access Controls	
Description	Provide controls to restrict users to authorized Single Sign-On transactions and functions	
Source	NIST SP 800-18	
Assumption	None	
Sub-requirements	4.6.1	Access controls prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion
	4.6.2	Access to security software is restricted to security administrators
	4.6.3	Inactive users' accounts are monitored and removed when not needed.
	4.6.4	Encryption when used, meets federal standards
	4.6.5	When encryption is used, there exist procedures for key generation, distribution, storage, use, destruction, and archiving
	4.6.6	Access is restricted to files at the logical view or field
	4.6.7	Access monitored to identify apparent security violations
	4.6.8	Controls exist to restrict remote access to the system
	4.6.9	Activity logs are maintained and reviewed
	4.6.10	The network connection automatically disconnects at the end of a session
	4.6.11	Guest and anonymous accounts, if used, are authorized and monitored
	4.6.12	An approved standardized log-on banner is displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished
	4.6.13	Sensitive data transmissions are encrypted
	4.6.14	A privacy policy is posted on the web site

Identifier	4.7	
Title	Audit Trails	
Description	Activity involving access to and modification of sensitive or critical Single Sign-On files is logged	
Source	NIST SP 800-18	
Assumption	None	
Sub-requirements	4.7.1	Audit trail(s) provides a trace of user actions
	4.7.2	Audit trail(s) can support after-the-fact investigations of how, when, and why normal operations ceased
	4.7.3	Access to online audit logs is strictly controlled
	4.7.4	Automated tools are available to review audit records in real time or near real time

Identifier	4.8 (Technical)	
Title	Access history	
Description	After successful login, a message with information about last successful login and how many unsuccessful login attempts have been made in the meanwhile must be displayed.	
Source	Best Practices	
Assumptions	None	
Sub-requirement	4.8.1	A login history must be provided.
	4.8.2	A logout history must be provided.
	4.8.3	A failed login history must be provided

Identifier	4.9 (Technical)	
Title	Access Restrictions	
Description	The Single Sign-On mechanism must offer the capability to define access rules.	
Source	Best Practices	
Sub-requirement	4.9.1	The Single-Sign-On mechanism must offer configurable access restrictions based on time.
	4.9.2	The Single-Sign-On mechanism must offer configurable access restrictions based on location.
	4.9.3	The Single-Sign-On mechanism must offer configurable access restrictions based on user-group.
	4.9.4	Access restriction criteria must be combinable.

5 Customer Care

Identifier	5.1	
Title	Non-student system access help	
Description	Provide system login/access support to non-student users	
Source	SFA Login/Access Survey	
Assumption	None	
Sub-requirements	5.1.1	Provide customer care support to 21,000 non-student Single Sign-On users
	5.1.2	Provide access support for 25,000 calls per month related to access

Identifier	5.2 (Technical)	
Title	Self-service and Customer Care	
Description	The Single Sign-On portal must provide tools for self-service and a contact for more complex problems.	
Source	Best Practices	
Assumptions	The Single Sign-On does not replace direct access to systems.	
Sub-requirements	5.2.1	If a password got lost a user can change users password by answering one or more security questions.
	5.2.2	A user must be able to change certain user-profile information via the self-service feature.
	5.2.3	Username changes can only be done through an Administrator
	5.2.4	Email Address changes can only be done through an Administrator.

6 Legal

Identifier	6.1	
Title	Provide privacy and confidentiality protections	
Description	Provide legal notices and protections for Privacy Act data and confidential data maintained within the Single Sign-On service	
Source	SFA Login/Access Survey	
Assumption	None	
Sub-requirements	6.1.1	Provide notices (i.e., banners) for Privacy Act
	6.1.2	Provide notices (i.e., banners) for confidential data

Identifier	6.2 (Technical)	
Title	Legal notice	
Description	A legal message must be displayed outlining the legal aspects of connecting to SFA systems through the Single Sign-On portal.	
Source	Best Practice	
Assumptions	None	
Sub-requirements	6.2.1	A message must be displayed explaining that the user leaves the Single Sign-On realm entering another system that has it's own security requirements.

7 Environment

Identifier	7.1 (Technical)	
Title	Supported operating systems	
Description	Provide the ability to support and integrate with a variety of operating systems.	
Sub-requirements	7.1.1	Windows NT
	7.1.2	Windows 2000
	7.1.3	Sun Solaris
	7.1.4	Hewlett-Packard Unix
	7.1.5	Linux
	7.1.6	Mainframe MVS
	7.1.7	VAX/VMS
	7.1.8	Mainframe OS 390
	7.1.9	Oracle

Identifier	7.2 (Technical)	
Title	Supported web servers	
Description	Provide support for major web servers.	
Sub-requirements	7.2.1	Apache
	7.2.2	Microsoft IIS
	7.2.3	IBM Http server
	7.2.4	iPlanet Enterprise Server

Identifier	7.3 (Technical)	
Title	Supported application server	
Description	Provide support for major application servers.	
Sub-requirements	7.3.1	Coldfusion
	7.3.2	Websphere
	7.3.3	JRUN
	7.3.4	Weblogic
	7.3.5	Citrix

Identifier	7.4 (Technical)	
Title	Supported proxy servers	
Description	Provide support for major proxy servers.	
Sub-requirements	7.4.1	CoolGen
	7.4.2	Apache
	7.4.3	Webcache

Identifier	7.5 (Technical)	
Title	User data storages	
Description	Provide support for major user data repositories	
Sub-requirements	7.5.1	LDAP v3
	7.5.2	Oracle DB
	7.5.3	Informix
	7.5.4	Microstrategy
	7.5.5	SQL databases
	7.5.6	RACF

8 Operations

Identifier	8.1	
Title	Administration	
Description	Administration is delegated	
Source	Best Practice	
Sub-requirements	8.1.1	Delegated administration must be configurable based on user groups.
	8.1.2	Group administration must be shareable between two or more administrators within the same-delegated administration group.

9 Audit and logging

Identifier	9.1 (Technical)	
Title	Audit capabilities	
Description	To allow for accountability logging and auditing must capture user actions.	
Source	Best Practices/Common Criteria	
Sub-requirements	9.1.1	The Single Sign-On mechanism must offer the option to define actions if certain events have taken place.
	9.1.2	The information that is captured and stored for audit must be configurable.
	9.1.3	The Single Sign-On mechanism must be able to detect abnormal user behavior and provide the ability to pass this data to intrusion detection systems must be provided.
	9.1.4	Audit tools must be available for authorized users, to review audit logs.
	9.1.5	The Administrator must be able to select specific security events.
	9.1.6	The Single Sign-On mechanism must be able to create and maintain a secure audit trail.
	9.1.7	Audit logs must be only available to authorized users.

10 Handling of Data

Identifier	10.1 (Technical)	
Title	Communication between systems and the Single Sign-On data store	
Description	The Single Sign-On solution must allow for secure communication between systems and the Single Sign-On data store.	
Source	Best Practices	
Assumptions	User data is synchronized between SFA systems and the Single Sign-On data store.	
Sub-requirements	10.1.1	Ensure encryption of Single Sign-On data.

Identifier	10.2 (Technical)	
Title	User data	
Description	Protection of confidential data must be ensured at all time.	
Source	Best Practices	
Sub-requirements	10.2.1	The Single Sign-On service must be able to provide secure web communication.
	10.2.2	Storage of confidential data must be done securely.

11 Performance and Scalability Requirements

Identifier	11.1 (Technical)
Title	Login response time
Description	The Single Sign-On infrastructure must support a login response time and session establishment time of at most 2 seconds with average load, and up to 5 seconds during peaks.
Source	Best Practices
Assumptions	The achievement of this performance goal depends on other components of the SFA infrastructure outside the scope of the project. Support of third party and remote sites may impose some additional delays, because of the number of redirections that may be necessary to establish a session with these external sites.

Identifier	11.2 (Technical)
Title	User self-service response time
Description	The Single Sign-On infrastructure must support a user self-service response time of 5 seconds.
Source	Best Practices
Assumptions	The achievement of this performance goal depends on other components of the SFA infrastructure and is outside the scope of the project.

Identifier	11.3 (Technical)
Title	Number of user self-service requests
Description	The Single Sign-On infrastructure must support an average of 1000 user self-service requests per day without any impact on performance.
Source	Best Practices
Assumptions	The achievement of this performance goal depends on other components of the SFA infrastructure and is outside the scope of the project.

Identifier	11.4 (Technical)	
Title	Users scalability	
Description	The Single Sign-On infrastructure must be able to support 23 million student users, and 25,000 school and financial partner users, without impacting system performance targets during average usage.	
Source	Best Practices	
Assumptions	This requirement critically depends on the design of the Single Sign-On access control data store.	
Sub-requirements	11.4.1	The infrastructure must be able to support 10,000 student concurrent logins without performance degradation.
	11.4.2	The infrastructure must be able to support 2,500 school, financial partner, employee, and operating partner concurrent logins without performance degradation.

12 Availability

Identifier	12.1 (Technical)	
Title	High availability (24x7)	
Description	The infrastructure must be designed for “high availability” with a 99.9% uptime.	
Source	Project scope	
Assumptions	Several dependencies on network and other infrastructure components.	
Sub-requirements	12.1.1	The infrastructure must feature no single point of failure, including network links.
	12.1.2	Support for redundant deployment with built-in fail-over capabilities, also across geographic locations.

Identifier	12.2 (Technical)	
Title	Technical Support	
Description	Technical support for Single Sign-On mechanism must be available.	
Source	Best Practices	
Assumptions	Users can still access the systems participating with Single Sign-On directly without going through the Single Sign-On portal.	

Identifier	12.3 (Technical)	
Title	Disaster recovery	
Description	After a major disaster, the Single Sign-On portal must be able to return to operational state in a timeframe consistent with the SFA disaster recovery procedures.	
Source	Best practice	
Assumption	Disaster recovery procedures are in place.	

Identifier	12.4 (Technical)
Title	Protection against data loss
Description	The Single Sign-On solution must be designed to allow for backup and recovery consistent with the SFA backup /recovery procedures.
Source	Best practice
Assumptions	Off-site media storage procedures, backup procedures and policies per capability are in place.

13 Security Requirements

Identifier	13.1	
Title	Auditable	
Description	Auditing involves recognizing, recording, storing and analyzing information related to security relevant activities. The resulting audit records can be examined to determine which security relevant activities took place and who is responsible for them.	
Source	Common Criteria/ISO15408	
Sub-requirements	13.1.1	Automatic response to events - Certain audit events (Incidents) must result in actions, which are executed automatically.
	13.1.2	Audit data generation - The level of which information is stored for audit, must be configurable.
	13.1.3	Audit analysis – Abnormal user behavior must be detected and the ability to pass this data to intrusion detection systems must be provided.
	13.1.4	Audit review – Audit tools must be available for authorized users, to review audit data.
	13.1.5	Audit event selection – The ability to select specific security events must be provided.
	13.1.6	Audit event storage – The ability to create and maintain a secure audit trail must be provided. Only authorized users are allowed to view or modify audit data.

Identifier	13.2	
Title	Secure Communication	
Description	Secure communication is concerned with assuring the identity of a party participating in a data exchange. This ensures that the originator cannot deny having sent the message, nor can the recipient deny having received it.	
Source	Common Criteria/ISO15408	
Sub-requirements	13.2.1	Non-repudiation of origin – The ability to verify if a communication request is originating from the system it claims to come from.
	13.2.2	Non-repudiation of receipt – The ability to verify if a system is the intended recipient for a communication request.

Identifier	13.3	
Title	Cryptographic support	
Description	Cryptography ensures that the following objectives are satisfied: identification and authentication, non-repudiation, trusted path, trusted channel and data separation.	
Source	Common Criteria/ISO15408	
Sub-requirements	13.3.1	Cryptographic key management – A key management function must be offered that allows the management of cryptographic keys throughout their lifecycle (generation through deletion).
	13.3.2	Cryptographic operation – Functions like strong encryption/decryption, cryptographic-checksum and secure hash must be offered.

Identifier	13.4	
Title	User data protection	
Description	User data must be protected from unauthorized access or manipulation.	
Source	Common Criteria/ISO15408	
Sub-requirements	13.4.1	Access control policy – Access to user data must be controlled and protected based on access policies.
	13.4.2	Access control functions – Access to user data is controlled by these functions, which are configured according to the access policies.
	13.4.3	Data authentication – Data authentication allows for verification of data if it has been forged or fraudulently modified.
	13.4.4	Export of user data – Security attributes associated with user data can be explicitly preserved or ignored when exporting user data.
	13.4.5	Information flow policy – Allow for read or write only access to user data for specific entities.
	13.4.6	Information flow control function – An Information flow control is provided based on the information flow policy allowing for users to read, write, modify, delete or create specific data.
	13.4.7	Import of user data – Security attributes associated with user data can be explicitly preserved or ignored when importing user data. This allows keeping access rights confidential if user data needs to be exported to other systems.

	13.4.8	Internal data transfer – User data protection is provided when data is transferred internally.
	13.4.9	Residual data protection – Ensure that deleted information is no longer accessible.
	13.4.10	Rollback – Offering an Undo for the last operation.
	13.4.11	Stored data integrity – Ensure that stored user data is protected from unauthorized access.
	13.4.12	User data confidentiality transfer protection – Ensure that user data is protected from unauthorized access during transfer between entities.
	13.4.13	User data integrity transfer protection – Ensure that user data is not manipulated during transfer between entities.

Identifier	13.5	
Title	Identification and authentication	
Description	Establish and verify a claimed user identity, to ensure that the right security attributes are associated.	
Source	Common Criteria/ISO15408	
Sub-requirements	13.5.1	Authentication failures – Actions (For example: A user is locked out after three unsuccessful login attempts) must be definable if a certain number of failed authentication attempts occur.
	13.5.2	User attribute definition – Each user has security attributes associated to him/her, which define users access rights appropriate to his/her role.
	13.5.3	Specification of secrets – Secrets (e.g. Password) must be checked against certain definable quality standards.
	13.5.4	User authentication – Offer a scalable robust authentication mechanisms.
	13.5.5	User identification – Before a user can take any actions, he/she has to be identified. Only exception is the login process.
	13.5.6	User subject binding – Processes accessing, changing or deleting objects are executed with the user’s security attributes.

Identifier	13.6	
Title	Security management	
Description	Management of security attributes of users allowing for separation of duties.	
Origin	Common Criteria/ISO15408	
Sub-requirements	13.6.1	Management of functions – Security functions must only be accessible by authorized users.
	13.6.2	Management of security attributes – Security attributes can only be modified, established or deleted by authorized users.
	13.6.3	Management of internal data – Audit, configuration or any other critical data must only be accessible by authorized users.
	13.6.4	Revocation – Security attributes must be revocable for each entity.
	13.6.5	Security attribute expiration – Security attributes must have a limited lifetime.

Identifier	13.7	
Title	Privacy	
Description	Protection against discovery and misuse of identity by other users.	
Source	Common Criteria/ISO15408	
Sub-requirements	13.7.1	Anonymity – A user can use a resource or service without disclosing the user’s identity to other users.
	13.7.2	Pseudonymity – A user’s identity is not disclosed to other users. But the user is still accountable for its action.
	13.7.3	Unlikability – A user can use a resource multiple times without other users being able to link these sessions to each other.
	13.7.4	Unobservability – A user can utilize a resource without other users or third parties being able to observe his/her actions or the usage.

Identifier	13.8	
Title	Protection	
Description	Ensure the integrity and manageability of the mechanism providing Single Sign-On functionality and all the data related to it.	
Source	Common Criteria/ISO15408	
Sub-requirements	13.8.1	Underlying abstract machine test – Functions, which are provided by the OS or the hardware platform, which the Single Sign-On mechanism relies on, need to be tested at start-up and on regular basis.
	13.8.2	Fail Secure – In the event of failures the Single Sign-On mechanism must go into a defined state.
	13.8.3	Availability of exported data – Critical data, which is exported to another IT product, must be still available for the Single Sign-On mechanism at the time of export.
	13.8.4	Confidentiality of exported data – Protection from unauthorized disclosure of data during transmission between the Single Sign-On mechanism and another IT product must be provided.
	13.8.5	Integrity of exported data - Protection from unauthorized modification of data during transmission between the Single Sign-On mechanism and another IT product.
	13.8.6	Internal data transfer – Protection of data transmitted between different pieces of the Single Sign-On mechanism must be provided.
	13.8.7	Physical protection – Restrictions on physical access to the Single Sign-On mechanism and the underlying hardware must be ensured.
	13.8.8	Trusted recovery – The Single Sign-On mechanism must start up in a controlled state.
	13.8.9	Replay detection – Replay of various entities (e.g. messages, service request, service responses) must be detected.
	13.8.10	Reference mediation – Before executing any action it must be evaluated against the security policies established for the specific user group and type of action.
	13.8.11	Domain separation – Security functions of the Single Sign-On mechanism must live in their own domain to avoid tempering.
	13.8.12	State synchrony protocol – State synchronization between the different parts of the Single Sign-On mechanism must be done with a secure exchange protocol.
	13.8.13	Timestamp – A reliable timestamp mechanism must be offered.

	13.8.14	Internal data consistency – Data must be consistent across the whole Single Sign-On mechanism.
	13.8.15	Internal data replication consistency – Data must be consistent between the Single Sign-On mechanism and the IT products utilizing the data provided by it.
	13.8.16	Self-test – The Single Sign-On mechanism must test itself when starting up and before users are allowed access.

Identifier	13.9	
Title	Resource Utilization	
Description	The Single Sign-On mechanism must provide mechanism to control resource utilization	
Source	Common Criteria/ISO15408	
Sub-requirements	13.9.1	Fault tolerance – In event of failures the Single Sign-On mechanism should maintain normal operation.
	13.9.2	Priority of service – High priority tasks cannot be interrupted by task with lower priority.
	13.9.3	Resource allocation – Use of resources by users and subjects is controlled to avoid a denial of service.

Identifier	13.10	
Title	Access and Session management	
Description	Controlling the establishment of a user’s session.	
Source	Common Criteria/ISO15408	
Sub-requirements	13.10.1	Scope of selectable attributes – Limit the scope of session security attributes that a user may select for a session.
	13.10.2	Limitation on multiple concurrent sessions – Users are only allowed a limited number of concurrent sessions.
	13.10.3	Session locking – Inactive sessions must be locked or closed.
	13.10.4	Access banner – An access banner must be present to display a configurable advisory warning message.
	13.10.5	Access history – Upon successful login, the user must be presented with a history of successful and unsuccessful attempts to access the user’s account.
	13.10.6	Session establishment – A function must be offered to define rules to deny access based on user location, time, credentials, authentication-method, etc.

Identifier	13.11	
Title	Trusted path/channels	
Description	Establish and maintain trusted communication between entities.	
Source	Common Criteria/ISO15408	
Sub-requirements	13.11.1	Secure transit of data – Confidential data must never be transmitted in the clear over any network connection, whether it is to/from internal or external systems.
	13.11.2	Trusted Path - Confidential data must never be transmitted in the clear between user and the single-sign-on mechanism.

3 Potential Alternatives

The potential alternatives listed in this section are an early observation; the next phase when approved and funded will analyze the requirements and recommend alternatives.

Custom Developed Single Sign-On Service

Implement a proprietary Single Sign-On service by developing user authentication business processes and policies that are enabled by a new technical capability that is owned, operated and maintained by SFA.

Business processes and IT enablers, which will require integration or definition, include:

- Logon and Session Establishment
- Application Access
- Logout and Session Termination
- Access Credential Administration (session timeout, credential suspension, credential revocation, credential reset)

Technologies to be considered for integration into a custom solution may include:

- SAML / XML
- SOAP
- LDAP
- RDBMS
- Encryption
- Web-based development tools (Java, C/C++, others as needed)
- Web application server (Websphere)
- Credential/Tokens (PKI, smart card, etc.)
- Web services (UDDI)
- Others as needed

Single Sign-on By Enhanced Current SFA Capability

Existing SFA business and technology capabilities may be reused with possible modifications and enhancements to provide a Single Sign-On service capable of meeting SFA requirements.

Business processes and IT enablers, which will require integration or definition, include:

- Logon and Session Establishment
- Application Access
- Logout and Session Termination
- Access Credential Administration (session timeout, credential suspension, credential revocation, credential reset)

Technologies to be considered for integration into an enhanced current SFA capability may include:

- SAML / XML
- LDAP

- RDBMS
- Encryption
- Web-based development tools (Java, C/C++, others as needed)
- Web application server (Websphere)
- Credential/Tokens (PKI, smart card, etc.)
- Others as needed

COTS enabled Single Sign-On Service

Implement a single sign-on service by integrating a commercial-off-the-shelf (COTS) system to SFA systems and user access control business processes.

Business processes and IT enablers, which will require integration or definition, include:

- Logon and Session Establishment
- Application Access
- Logout and Session Termination
- Access Credential Administration (session timeout, credential suspension, credential revocation, credential reset)

Solution vendors may include the following firms:

- Waveset (Lighthouse)
- Thor Technologies
- Access360
- Netegrity (Siteminder)
- Entrust (getAccess)
- Tivoli (Policy Director)
- Oblix
- Securant
- Computer Associates
- BMC Software

Single Sign-On Service from a Managed Service Provider

Implement a Single Sign-On service by outsourcing user authentication processes to a managed service provider specializing in system access control integration and operations.

Business processes and IT enablers, which will require integration or definition, include:

- Logon and Session Establishment
- Application Access
- Logout and Session Termination
- Access Credential Administration (session timeout, credential suspension, credential revocation, credential reset)

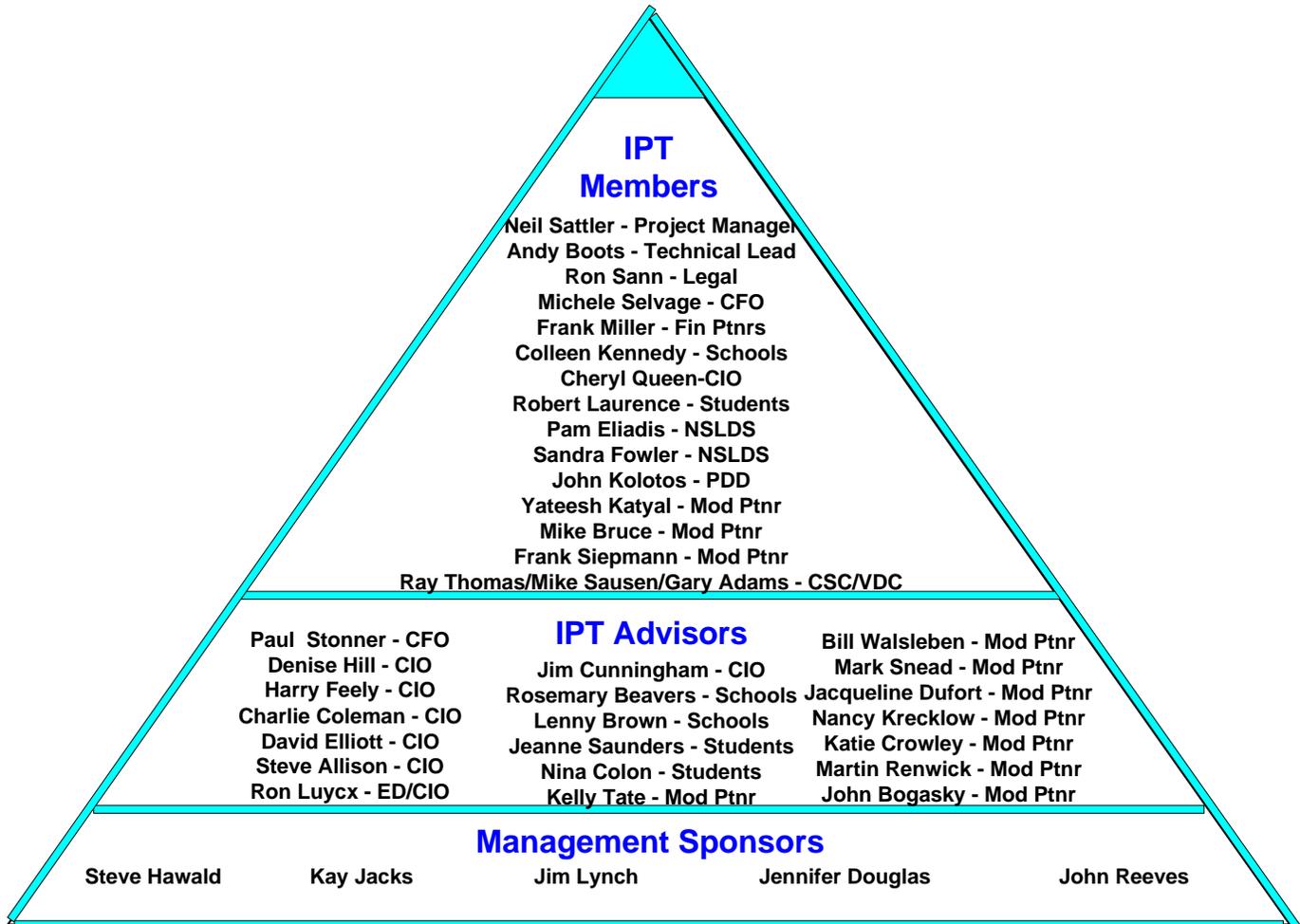
Managed Service Providers may include the following:

- Microsoft Passport/.NET Services
- Sun Microsystems (Liberty Alliance)
- AOL (Magic Carpet)

- Aventail
- Jamcracker
- VeriSign

Appendices

Appendix A: IPT team



Appendix B: Acronyms and Abbreviations

Acronym	Definition
API	Application Program Interface
CB	Campus-Based
CBS	Campus-Based System
COD	Common Origination and Disbursement
COTS	Commercial Off-the-Shelf (Software)
CRM	Customer Relations Management
CPS	Common Processing System
DLOS	DL originations and disbursement
EAI	Enterprise Architecture Infrastructure
ECB	eCampus Based
ED	US Department of Education
EDCAPS	US Department of Education Consolidated Accounting and Payment System (ED/OCFO)
EDConnect	EDConnect software
FAFSA	Free Application for Federal Student Aid
FISAP	Fiscal Operations Report and Application to Participate
FMS	Financial Management System
GAPS	Grant Administration Payment System (subsystem of EDCAPS)
IFAP	Information for Financial Aid Professionals
IPT	Integrated Product Team
IDS	Intrusion Detection System
NSLDS	National Student Loan Data System (Raytheon)
PEPS	Postsecondary Education Participants System
PPA	Program Participation Agreement
RFMS	Pell originations & disbursement
RDBMS	Relational Database Management System
SAIG	Student Aid Internet Gateway
SAR	Student Aid Report
SFA	Student Financial Assistance
Single Sign-On	Single Sign-On
TIVWAN	Title IV Wide Area Network
VDC	Virtual Data Center

Appendix C: SFA Login/Access Survey Results and Summary

See Attached MSEXcel File - 82.1.2 SFA Logon Access Survey - Requirement Definition Draft.xls