



SFA Modernization Partner
United States Department of Education
Student Financial Assistance

Business Technology Alignment

SFA Technology Policy Guide

Version 2.0

Task Order #85
Deliverable # 85.1.2



CHANGE LOG					
Suggested Changes/Comments	Page	Author	Date	Change Made Y/N	Comment



TABLE OF CONTENTS

1	<i>Introduction</i>	1
1.1	Using this Guide	1
1.2	Sources of Standards and Policies	1
1.3	Authority and Governance.....	2
2	<i>Conceptual Architecture</i>	2
3	<i>Technical Reference Model</i>	3
4	<i>Technology Policies and Standards</i>	5
4.1	User Interface Services	6
4.2	Application Services	9
4.3	Enterprise Data Management.....	15
4.4	Distributed Computing	21
4.5	Data Interchange	25
4.6	Network Services	28
4.7	Operating Systems	33
4.8	Systems Management	37
4.9	Security Services.....	42
4.10	External Environment	52
5	<i>Appendices</i>	55
	<i>Appendix A: Acronyms</i>	56
	<i>Appendix B: Quick Reference Guide</i>	58
	<i>Appendix C: Sources Referenced</i>	64



1 INTRODUCTION

This document serves as a reference tool for SFA technical architects, system administrators, developers, information technology executives, and others that require guidance on implementing SFA technical standards and policies.

1.1 Using this Guide

The *SFA Technology Policy Guide* is divided into technology groups, including User Interface Services, Application Services, Enterprise Data Management, Distributed Computing, Data Interchange, Network Services, Operating Systems, System Management, Security Services, and external environments. The follow information is provided for each service in a technology group:

- *Brief Description* defines a service and describes what functions the service performs.
- *Target Standards* are listed in a table which contains the current and planned SFA solution standards.
- *Approved Standards* provides a detailed description of policy underlying a standard and the rationale for the selection of a standard.

1.2 Sources of Standards and Policies

The technology policies and standards are established through the U.S. Department of Education Student Financial Assistance (SFA) modernization effort. The SFA architecture is based on The Open Group Architectural Framework (TOGAF) which defines a process for developing an architecture and describes the fundamental technologies in the architecture.

Both open systems standards and proprietary standards are employed by SFA. Open systems products and technologies are designed to use open interfaces with specifications that are readily available to the public and revisions with timely notice through a public process. Proprietary standards are not publicly available, and they may be implemented through commercial off the shelf (COTS) products or developed by SFA.

SFA strives to comply with external policies and standards as established in legislation or federal government policy. To be in compliance with Clinger-Cohen legislation and Office of Management and Budget (OMB) guidance, an SFA information technology architecture will contain an Enterprise Architecture, a Technical Reference Model (TRM), and a Standards Profile. This Technology Policy Guide contains the TRM and Standards Profile that provide compliance.



1.3 Authority and Governance

The authority for this Technology Policy Guide comes from the SFA Chief Information Officer through the Information Technology (IT) Management organization. The roles, responsibilities, and IT decision-making processes within SFA—collectively referred to as Enterprise Architecture Management (EAM)—are detailed in Section 8 of the *SFA Information Technology Architecture Framework - Phase I* document.

2 CONCEPTUAL ARCHITECTURE

This *Technology Policy Guide* is written to complement the SFA Information Technology Architecture (ITA). The ITA provides the framework of principles and practices that direct the design, construction, deployment, and management of information technology and systems (from *Enterprise Information Technology Architecture Framework: Business Drivers and Architecture Principles* October 8, 1998). The ITA guiding principles are:

The architecture must support the business. The enterprise architecture and standards will be designed to (1) support and optimise SFA operations, (2) be highly flexible to accommodate future business changes, and (3) help ensure the overall success of the SFA business.

Reengineer business processes and supporting IT together. New information systems will be implemented after work processes have been analysed, simplified, or otherwise redesigned as appropriate, in compliance with Clinger-Cohen legislation and Raines' rules.

Enhance and simplify access to information. Timely access to information through the tools and applications required to access and manipulate that information will be available to all individuals unless there is a specific, compelling reason to restrict access.

Design integration and reuse into IT initiatives. SFA IT initiatives will be designed to maximize reuse of existing code and databases.

Use industry-proven technology. IT applications and technical infrastructure decisions must be based on industry-proven and supported components, methods, standards, and tools consistent with industry technological and market direction.

Maintain vendor neutrality. Standards and technology choices will be based on vendor-neutral standards where they are available and realistically can be implemented. Products will be chosen from any vendor that has strong business stability, provides the best technology and service for a business need, and whose products are compliant with architecture standards.



Solutions preference. When most cost effective and beneficial, SFA’s solutions preference will be (1) outsourcing, (2) commercial-off-the-shelf (COTS) products, (3) reuse of existing applications, and (4) custom applications.

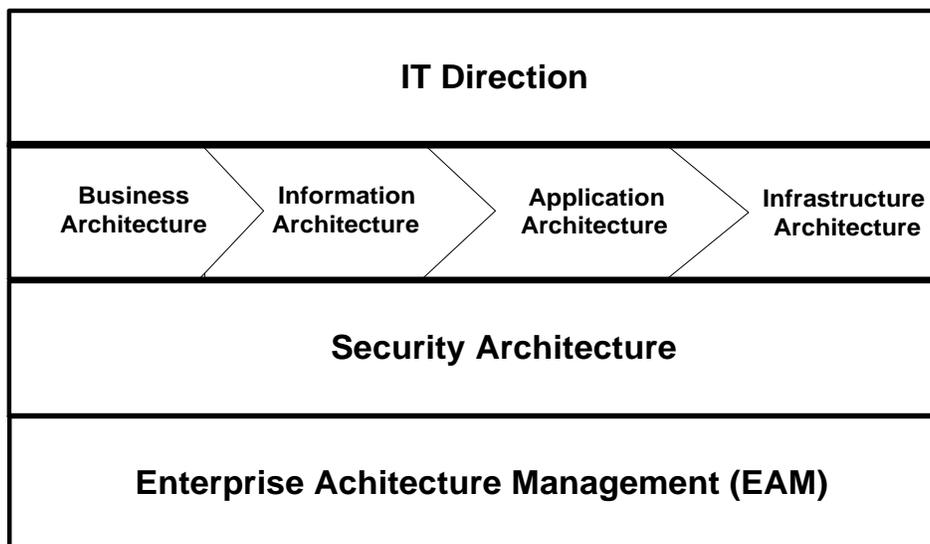
Reduce integration complexity. Products, tools, designs, applications, and methods will be selected to reduce integration and infrastructure complexity.

Architecture enforcement. The information systems and technology infrastructure implemented by SFA will be compliant with the SFA Enterprise Architecture and Common Operating Environment (COE).

Periodic architecture review, alignment, and refreshment: The ITA will be periodically reviewed (at least annually) and updated according to a disciplined, structured maintenance and technology refreshment process. This structure will include a configuration management process and supporting tools.

The SFA target ITA is composed of seven structural elements. These components form an integrated enterprise architecture designed to link the IT functions with the business goals. Exhibit 2-1 shows the infrastructure architecture and management functions and how they provide the foundation for the IT direction.

Exhibit 2-1: IT Components



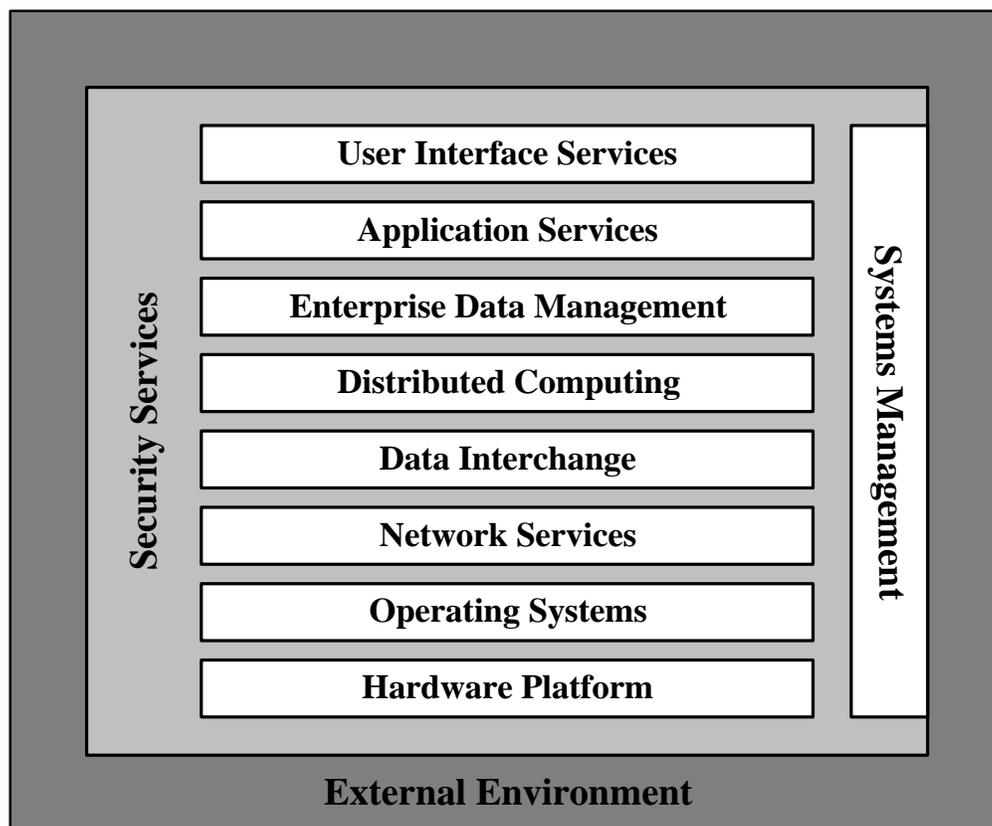
3 TECHNICAL REFERENCE MODEL

The basis for the Technology Policy Guide is the Technical Reference Model (TRM), which is a conceptual representation of services and interfaces in the information system. The TRM



provides a context for understanding how the various technologies required to implement information management relate to each other. This Technology Policy Guide is based on the TRM. The SFA TRM is depicted in Exhibit 3-1.

Exhibit 3-1: Technical Reference Model



The major service areas in the SFA TRM are:

User Interface Services—technologies that permit users to interact with applications, including web-enabled applications.

Application Services—technologies that support SFA users in performing the business processes of the organization.

Enterprise Data Management—technologies for managing SFA’s common and unique data definitions for use across systems.

Distributed Computing—technologies that allow computing services to operate similarly across physically and even geographically dispersed applications.

Data Interchange—technologies enabling exchange of data between different platforms.



Network Services—technologies enabling transfer of messages and data over a network.

Operating Systems—technologies that enable computers to manage resources and memory and execute applications.

Hardware Platform—physical components that provide the essential computing capabilities in the information systems architecture, generally categorized as desktop computers, workstations, servers, and mainframe systems.

Security Services—technologies and practices that protect SFA information assets. Security services are integrated into each major service area.

Systems Management—technologies and practices that enable the monitoring and control of the SFA information technology infrastructure. Systems management is influenced by every other service area.

External Environment—infrastructure technologies supporting the transfer of information but not part of the hierarchical structure of the TRM. The external environment influences every major service area.

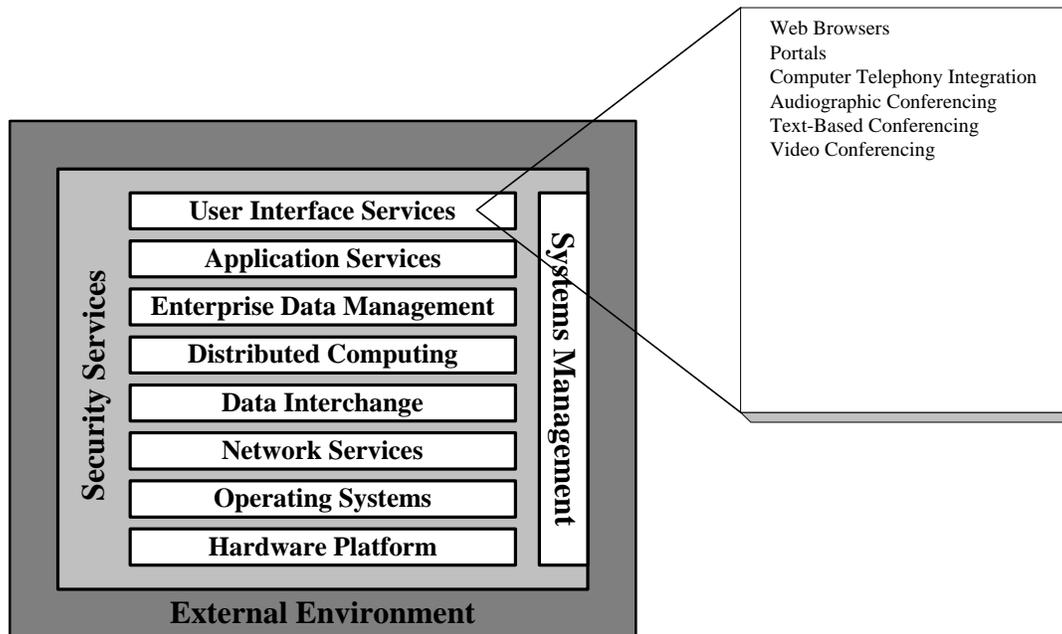
4 TECHNOLOGY POLICIES AND STANDARDS

This section is divided into the major service areas of the architecture. For each major service area, four aspects are detailed: a general description, the standard solution, a description of the technology policy, and a rationale for the standard.

Each technology policy and standard will have a timeline table defining the standard products used by SFA now and those slated to be used in the future. The timeline will be updated quarterly to reflect changes in SFA business objectives and emerging technologies.



4.1 User Interface Services



Brief Description

User interface services determine how users interact with an application from a software perspective. Depending on the capabilities required by users and the applications, these interfaces may include the following:

- *Web browsers* are client applications that provide an user interface by rendering Hypertext Markup Language (HTML) documents. They allowing users to view and interact with applications and documents containing text, graphics, audio, and other content. Web browsers also provide support for navigation within and across documents through the use of embedded hyperlinks. Technologies such as Java allow users to interact with existing legacy applications through web browsers.
- *Portals* provide a web-based user-customizable point of access to a wide variety of content, documents, and applications. A portal provides integrated access, authorization, and authentication to SFA services through the web.
- *Computer Telephony Integration (CTI)* merges computers, networks, PBX switches, PC-based answering machines, faxes, and pagers. CTI enables automated handling of telephone calls, automatic call back, initiation of workflow, a high quality of service for customers, and sophisticated task tracking.



- *Audio Graphic Conferencing* provides a cost-effective method of conferencing when seeing the conference participants is not essential. The audio is typically a telephone conference call, and an whiteboard image is provided over the network that can be modified by all participants. The whiteboard enables collaboration beyond a telephone conference call.
- *Text-Based Conferencing* allows conference participants to view each others text input. One of the features of the text-based conference is that the text can be saved and referred to at a later time. It requires the lowest network bandwidth of the three types of conferencing described.
- *Video Conferencing* enables people at different sites to simulate face-to-face meetings in real time. Current video conferencing options range from stationary systems installed in dedicated video conferencing rooms to personal computer video units. In addition to voice and video, video conferencing systems may enable the sharing of graphics and electronic documents. Personal computer video conferencing links individuals rather than groups.

Target Standards

Target Standards: User Interface

	FY 2002	FY 2003	FY 2004
Web Browsers			
	HTML v4.0	HTML v4.0	HTML v4.0
	HTTP v1.0	HTTP v1.0	HTTP v1.0
Portals			
	Viador E-Portal Suite v6.1.1	WebSphere Custom Components	WebSphere Custom Components
Computer Telephony Integration			
	TBD	TBD	TBD
Audio Graphic Conferencing			
	TBD	TBD	TBD
Text-Based Conferencing			
	TBD	TBD	TBD
Video Conferencing			
	TBD	TBD	TBD



Approved Standards

Web Browsers – HTML v4.0, HTTP v1.0

Description: SFA web browser services will provide server communication, communication security, Section 508 accessibility, presentation services, scripting, and run-time services. SFA products should support HTML and Java technologies.

Rationale: For external users accessing SFA information via a web browser, SFA language and protocol standards are HTML v4.0 and HTTP v1.0. SFA customers will use a variety of browsers, including text-based browsers such as Lynx. Support does not imply full functionality of features that are available only with more recent standards of products.

Portals – Viador E-Portal Suite v6.1.1

Description: Portal technology will provide a single point of access to SFA data and will be implemented with the Viador E-Portal Suite to provide the portal services.

Rationale: No published industry standard identified.

Computer Telephony Integration – TBD

Description: SFA is developing its customer relationship management (CRM) strategy, which will include CTI. There are presently a variety of solutions spread across multiple call centers.

Rationale: Industry standards vary by platform; more detail will be provided as the standards are selected.

Audio Graphic Conferencing – TBD

Description: To be determined.

Rationale: Multiple industry standards exist. No recommendation has been made.



Text-Based Conferencing – TBD

Description: To be determined.

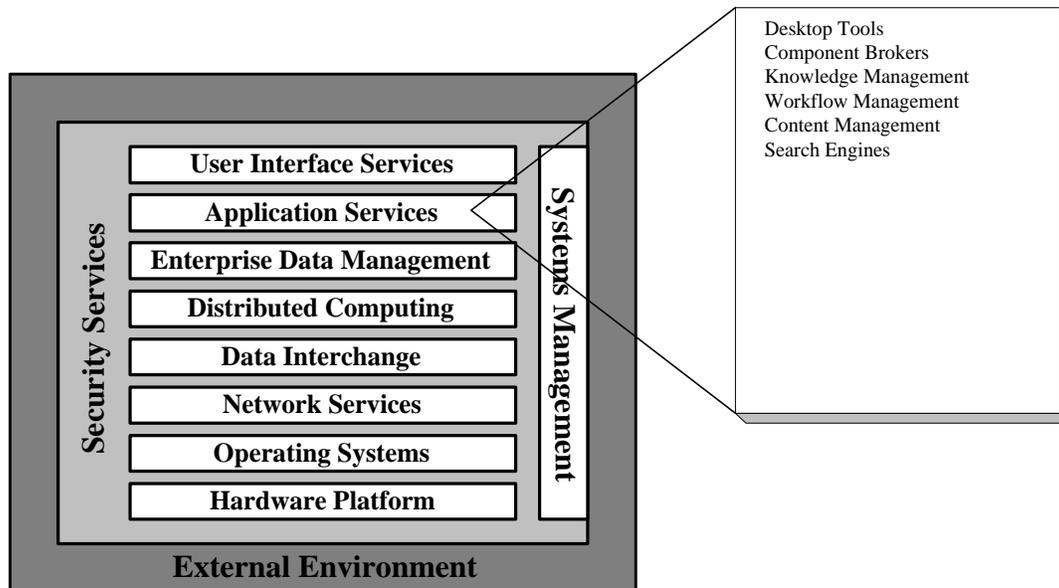
Rationale: Multiple industry standards exist. No recommendation has been made.

Video Conferencing – TBD

Description: To be determined.

Rationale: Multiple industry standards exist. No recommendation has been made.

4.2 Application Services



Brief Descriptions

Application services provide support for the business processes of an organization, including transaction services and software development environments. These services also enable an organization to deploy network-centric applications in the internet and intranet environments encompassing both application server services and web server services.



Software development for SFA applications will utilize a variety of tools, processes, and methodologies. Standards for these are given in the *SFA Software Engineering Handbook*.

The SFA Desktop COE, cited in this and following sections, is defined as the commercial-off-the-shelf (COTS) products and applications supported by the Microsoft Office 2000 suite of products in the current SFA Seat Management project.

- *Desktop Tools* are office productivity applications that support a standard office automation environment. They include user interface, word processing, spreadsheets, presentation graphics, and web browsers.
- *Component Brokers* provide object-based functionality to the application server. An object-based capability provides a standard model for object state and behavior accessible through object methods. A component broker provides a scalable, manageable environment for developing and deploying distributed component-based solutions. The component broker is an object server that includes a development environment that is optimized for creating business objects that run in the component broker server. This server consists of both a run-time package and a development environment.
- *Knowledge Management* provides information search and retrieval capability. These services offer various search types on different data groups, such as unstructured digital information, structured data, word processing documents, HTML-based files, e-mail messages, and electronic news feeds.
- *Workflow Management* facilitates work-related processes within an organization and often supports relatively static business processes, such as purchase order and claims processing. Workflow management creates run-time options by navigating through previously defined workflow models. Applications are invoked automatically, and work items are created and distributed to the people involved. Mail systems, groupware tools, and electronic forms packages can provide some workflow functionality.
- *Content Management* manages web site content delivery from the development environment to the production environment. The content management component provides the following services:

Authoring—allows users to associate and launch development applications against the content managed by the component.

Versioning—maintains versions of each individual web site artefact. The individual content versions are associated with web site configurations or releases.

Categorization and Publishing—manages groups of content artefacts according to user-defined criteria and supports publishing of these content artefacts.

Development Collaboration and Workflow—provides process control and related methods that support collaboration between personnel in the development



community and the production community. The collaboration and workflow utilities provide a methodical way to ensure that content change is appropriately authorized.

Integration of Multiple File Types—supports any type of file.

Summarization—produces a summary report of a configuration or release and the web site artefacts that were delivered from the development environment to the production environment.

- *Search Engines* provide search and retrieval capability on different data sets in an internet based environment.
- *Application Specific Standards* for MQ Series Applications are described in Appendix ff.

Target Standards

Target Standards: Application Services

	FY 2002	FY 2003	FY 2004
Desktop Tools			
	MS Office2000 Professional	MS Office2000 Professional	MS Office Professional
	MS Internet Explorer 5.5	MS Internet Explorer 5.5	MS Internet Explorer 5.5
Component Broker			
	IBM WebSphere/IOP	IBM WebSphere/IOP	IBM WebSphere/IOP
Knowledge Management			
	Autonomy Knowledge Suite v3.1	Autonomy Knowledge Suite v3.1	Autonomy Knowledge Suite v3.1
Workflow Management			
	MQ Series Workflow v3.2.2	MQ Series Workflow v3.2.2	MQ Series Workflow v3.2.2
Content Management:			
	Interwoven Teamsite v4.2.1	Interwoven Teamsite v4.2.1	Interwoven Teamsite v4.2.1
Search Engine:			
	Autonomy Knowledge Suite v3.1	Autonomy Knowledge Suite v3.1	Autonomy Knowledge Suite v3.1



Approved Standards

Desktop Tools – MS Office 2000 Professional, MS Internet Explorer 5.5

Description: Desktop tools will be specified in the SFA Desktop COE. The SFA standard office productivity tools consist of programs for word processing, spreadsheet, and presentation graphics.. Software products that are designed to international or national standards are preferred over those designed to a lower standard. Additionally, COTS software is always preferred over government-off-the-shelf (GOTS) software produced by other federal agencies or private companies working under contract for the government.

Rationale: Standards for common office productivity tools are typically defined by de facto industry file formats. File formats are formal structures of file records and layouts that are recognizable and usable by various related products. As a product utility becomes prominent in the industry, other tools and products tend to include the capability to access, use, and create files in the same format as those used by the prominent product. Common file formats for standard office and other productivity tools are given in the table below.

Document Type	Standard/Vendor Format	Recommended File Name Extension
Plain Text	ASCII Text	.txt
Compound	Acrobat	.pdf
Document	HTML	.htm
	MS Word	.doc
	Rich Text Format	.rtf
Presentation	MS PowerPoint	.ppt
Spreadsheet	MS Excel	.xls
Graphics	CGM	
	JFIF	
	GIF	.gif
Audio	Wave (WAV)	.wav
	Audio-Video Interleaved	.avi
	Audio UNIX (AU)	
Video	MPEG, MPEG2	.mpe
	Real Video	.rm, .ram



Internet	HTML	.htm
Compressed	WINZip	.zip
Database	Dbase	.dbf
	MS Access	.mdb

Component Broker – IBM WebSphere/IIOP

Description: The SFA component broker application will transparently provide a number of services to business objects or enterprise beans, including concurrency control, event, notification, externalization, identity, naming, transaction, query, and security services. The component broker run-time environment will support the execution of C++ and Java-based business logic that follows the CORBA 2.0 model or the EJB 1.0 specification.

Rationale: SFA component broker standards will comply with the open standards contained in the Object Management Group's (OMG) Common Object Request Broker Architecture (CORBA) initiative and the Component Broker Managed Object Framework (MOFW).

Knowledge Management – Autonomy Knowledge Suite v3.1

Description: The SFA knowledge management function, in conjunction with the search engine function, will provide a technology infrastructure for the automatic exploitation of content. This will provide the ability to use various types of information searches and personalized profiling and features to search both structured and unstructured data. The SFA product will support a thesaurus query if a thesaurus is loaded into the environment.

Rationale: No published industry standard identified..

Workflow Management – MQ Series Workflow v3.2.2

Description: Workflow management will be used by SFA to design, document, execute, control, improve, and optimize the business processes. SFA will leverage the workflow management tools to provide the following:

- Core components of the enterprise architecture through integration of business processes across enterprises by acting as a workflow broker.
- Integration of existing CICS applications to power e-business solutions



- Management of fully automated application-to-application workflow
- Management of workflow processes, including applications that require human intervention
- Web browser support with rapid application integration capability
- Scalability from Windows NT up to IBM OS/390 servers

Rationale: No workflow management standards currently exist, but the Workflow Management Coalition (WfMC) is defining standard interfaces between workflow engines, workflow definition packages, management information tools, work list tools, and invoked applications. SFA workflow applications should use high-level application programming interfaces (APIs) to communicate with desktop applications and use industry-standard relational databases as their data store.

Content Management – Interwoven Teamsite v4.2.1

Description: Content management will accelerate the way SFA delivers its business to the web, leveraging appropriate resources at all levels of the organization. Distributed control over content creation and deployment will shorten the launch cycle by enabling the management of the process. Content management will include replication and syndication features with rules-based distribution of all content across the SFA network. It will manage numerous deployment rules for SFA web sites. These deployment rules will support automated processes such as one-button publishing and transformation processes such as deployment to web configurations.

Rationale: No industry standard is established.

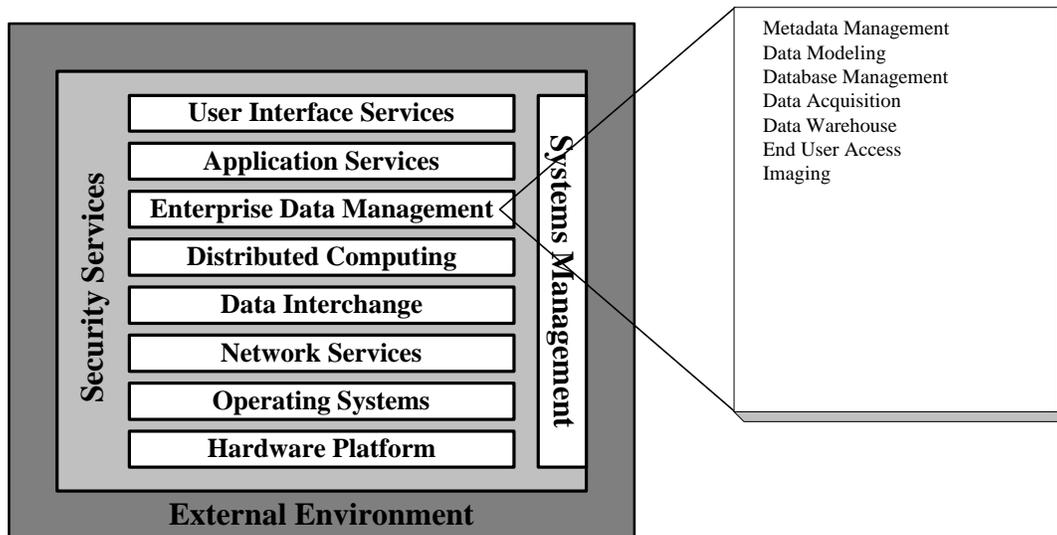
Search Engine – Autonomy Knowledge Suite v3.1

Description: The search engine will provide pattern-matching technology that will enable SFA to efficiently identify and encode unique key words within text documents. The search engine will then locate and retrieve content, such as a set of web sites, news feed, or an e-mail archive that match the search parameters.

Rationale: No published industry standard identified.



4.3 Enterprise Data Management



Brief Descriptions

Management of data is central to all systems. It encompasses the creation, storage, retrieval, use, maintenance, and deletion of data. Enterprise data management services include:

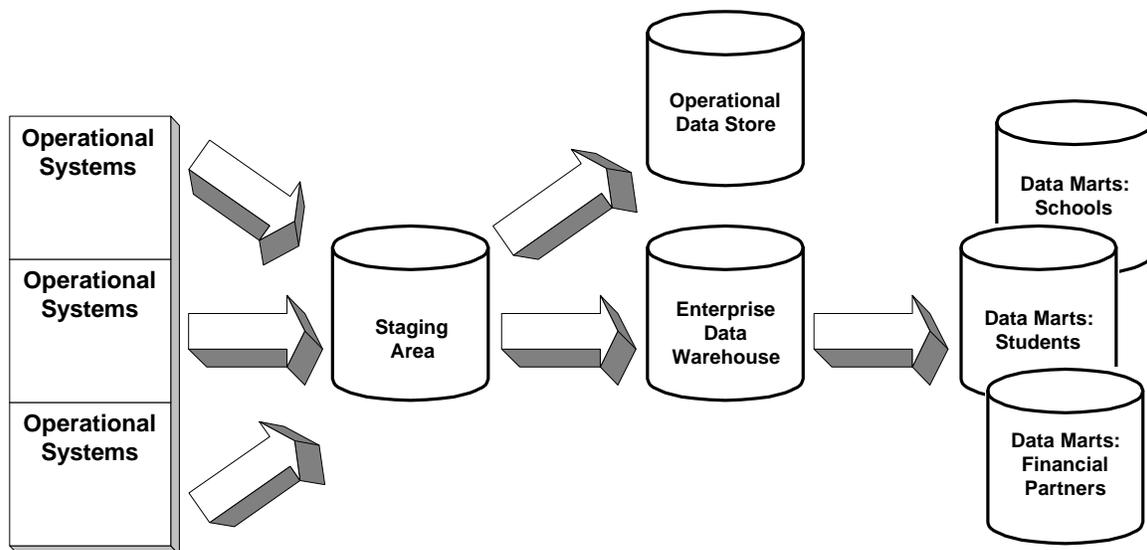
- *Metadata Management* allows data administrators and information engineers to access and modify data about data (i.e., metadata). Metadata can include internal and external formats, standard definitions, integrity and security rules, and location within a system. Enterprise data dictionary and repository services also allow end users and applications developers to recommend new data structures or changes to standardized data structures and to obtain logical data structures that will be implemented in the enterprise databases. Data administration defines the standardization and registration of entities (equivalent to tables or files) and attributes (equivalent to columns or data elements) to meet the requirements for data sharing and interoperability among information systems throughout the enterprise. Data administration functions include procedures, guidelines, and methods for effective data planning, analysis, standards, modeling, configuration management, storage, retrieval, protection, validation, and documentation. The enterprise data dictionary supports data definitions that are used to create data structures in different database management systems (DBMSs).
- *Data Modeling* identifies and clearly defines the entities in which the business must keep data and the important associations between those entities. Resolving differences in conflicting meanings, states, business rules, or names by building the data model enables meaningful progress toward developing shared, subject-oriented databases that can greatly reduce information float, redundant work, data and programming, and excessive time and cost in



conducting the business. A conceptual data model lays the foundation for building shared databases and for reengineering the business.

- *Database Management System (DBMS)* provides controlled access to standardized enterprise data. To manage the data, the DBMS provides concurrency control and facilities to combine data from different schemas. DBMS services provide support to different data implementations, including relational, hierarchical, network, object-oriented and flat-file data structures. A relational database management system (RDBMS) is a software system that manages data using the relational model. The relational model conceptually stores data in two-dimensional tables that consist of columns and rows. Tables are related to each other using a primary/foreign key mechanism. Some of the functions performed by the RDBMS are transactional concurrency, backup and recovery, security, enforcement of data integrity, and support for data manipulation. DBMS services are accessible through a programming language interface, an interactive data manipulation language interface such as SQL, or an interactive/fourth-generation language interface.
- *Data Acquisition* services allow the data warehouse data marts and operational data store to draw data from many different types of operational systems. The elements of the data acquisition services are access to source data, the data warehouse architecture, and end user access. Exhibit 4-1 depicts the flow of data in the data warehouse architecture from the data sources to the data marts.

Exhibit 4-1: Data Acquisition



The source data are the data collected and stored by operational and online transactional processing (OLTP) business applications. Understanding where data is stored across the enterprise is a key component for developing and maintaining data warehouses and data marts. SFA source data will come from the DBMS, legacy systems, enterprise resource planning (ERP) systems, and external sources.



- *Data Warehouse* services provide read-only, time-dependent data for end user access, online analysis, and reporting. This is after extract, transform, and load (ETL) procedures. The data warehouse is the point of integration between the enterprise ETL and the ETL feeding the data marts. The data warehouse architecture encompasses the hardware and software that support the processing, storage, and access of data as it flows from the source to the end user. The major data stores within the SFA data warehouse architecture are:

Staging—a temporary area in which data is staged for transformation and loading into the data warehouse.

Data Warehouse—an integrated and centralized data store organized for end user reporting and analytical access.

Operational Data Store—the storage of detailed transaction data in a normalized format for operational reporting. Transactions focused with no historical data (data update characteristic of “overwrite” data fields).

Data Marts—subject groupings by business area or data area.

- *End User Access* services provide the mechanisms and architecture to access and display data in an understandable and flexible way to the end user. There are multiple ways to move data from the source to the end users, depending on requirements. Access mechanisms include query and reporting tools, online analytical processing (OLAP) tools, and data mining and knowledge discovery. With end user access, appropriate security controls must be considered.
- *Imaging* services provide data acquisition through scanning of print documents so they can be archived in electronic format.

SFA will create an enterprise data model containing standard data structures of metadata for data that can be shared across the enterprise. All new development will use data definitions and structures in the Enterprise Data Model for shared data. All new development will use the SFA standard naming conventions and metadata content. The Enterprise Data Management Group will maintain both mappings (to be detailed in *SFA Data Management Policies and Procedures*).

Target Standards

Target Standards: Enterprise Data Management

	FY 2002	FY 2003	FY 2004
Metadata Management	ISO 11179	ISO 11179	ISO 11179



Data Modeling			
	Sybase Power Designer 7.0	Sybase Power Designer 7.0	Sybase Power Designer 7.0
	Sterling Software CoolGen	Sterling Software CoolGen	
	Rational Suite 1.5 (Rose)	Rational Suite 1.5 (Rose)	Rational Suite 1.5 (Rose)
Database Management (Mod System & Data Mart)			
	Oracle 8i/8.05	Oracle 9i	Oracle 9i
	DB2	DB2	
Data Acquisition (Data Mart)			
	Informatica Power Center Server 1.7	Informatica Power Center Server 1.7	Informatica Power Center Server 1.7
Data Warehouse			
	MicroStrategy 7.0	MicroStrategy 7.0	MicroStrategy 7.0
End User Access (Data Mart)			
	Intelligence Server 7.0	Intelligence Server 7.0	Intelligence Server 7.0
	Web 7.0	Web 7.0	Web 7.0
	Broadcaster 6.5	Broadcaster 6.5	Broadcaster 6.5
	InfoCenter 6.5	InfoCenter 6.5	InfoCenter 6.5
	Agent 6.5	Agent 6.5	Agent 6.5
Imaging			
	TBD	TBD	TBD

Approved Standards

Metadata Management – ISO 11179

Description: SFA metadata management will represent an enterprise-wide definition of shared data. SFA’s metadata management services will provide the ability to:

- Track traditional metadata, such as file structure definitions, database field names, and lengths and standards found in a data model.
- Manage technical metadata, such as field-to-field mappings between source and target and query response times.
- Store business metadata, such as business rules describing what is and is not included within the data warehouse and definitions of business hierarchies and KPIs.

The metadata management services will include a metadata repository. The metadata repository will contain detailed information on the data warehouse tables, attributes, facts, and relationships. This central data



repository will allow for reports to be created once and deployed through the Micro Strategy applications.

Rationale: SFA metadata management will comply with the ISO 11179 standard.

Data Modeling – Sybase Power Designer 7.0, Rational Suite 1.5 (Rose)

Description: Data modeling will support *object-relational* database application design. In addition to automating the design, maintenance, and recovery of back-end relational database applications, data modeling will help SFA design the user-defined data types to be stored in their database, as well as the business logic used to access and manipulate database information. Data modeling technology will allow SFA to import existing information into class diagrams and import a database SQL script into a physical data model, or recover an existing database through an ODBC connection.

Rationale: No published industry standard identified.

Database Management (Mod System & Data Mart) – Oracle 8i/8.05, DB2

Description: All new development will be based on relational database management systems.

Rationale: The SFA standard is an object-relational database conforming to the SQL 92 standard. This type of database is a relational database that supports the object operation. SFA will use SQL and some extensions to support the objects; this will provide backward compatibility to previous releases. SFA has selected Oracle 8i (mid-tier) and DB2 (mainframe) as its database standards.

Data Acquisition (Data Mart) – Informatica Power Center Server 1.7

Description: SFA will implement an ETL tool with its own global meta-repository and its own server. SFA will use an engine-based approach to access source data, and all data extraction will be via the SFA ETL process.



Rationale: The industry has not agreed on a single set of standards for products used to populate a data warehouse. The Informatica Power Center tool will populate the SFA data warehouse.

Data Warehouse – MicroStrategy 7.0

Description: The SFA data warehouse architecture will provide a single point of integration for all SFA data. The SFA enterprise data warehouse will be built using a star or snowflake schema. SFA will use Micro Strategy products for end user access to the data warehouse. SFA is currently identifying additional query tools to enhance query and reporting capabilities.

Rationale: The SFA data warehouse will conform to the SQL 92 standard.

End User Access (Data Mart) – Intelligence Server 7.0, Web 7.0, Broadcaster 6.5, InfoCenter 6.5, Agent 6.5

Description: SFA will use Micro Strategy OLAP tools to provide end user access to the enterprise data warehouse and data marts. The following table lists these tools and their functions:

Product	Function
Intelligence Server 7.0	ROLAP report delivery (mid-tier)
Web 7.0	ROLAP analysis over the Web
Broadcaster 6.5	Report broadcasting
InfoCenter 6.5	Subscription and publishing Web portal
Agent 6.5	Client workstation application

Rationale: No published industry standard identified.

Imaging– TBD

Description: SFA currently has several imaging systems in place. While there is no standard for the manner in which imaging services acquires document data,

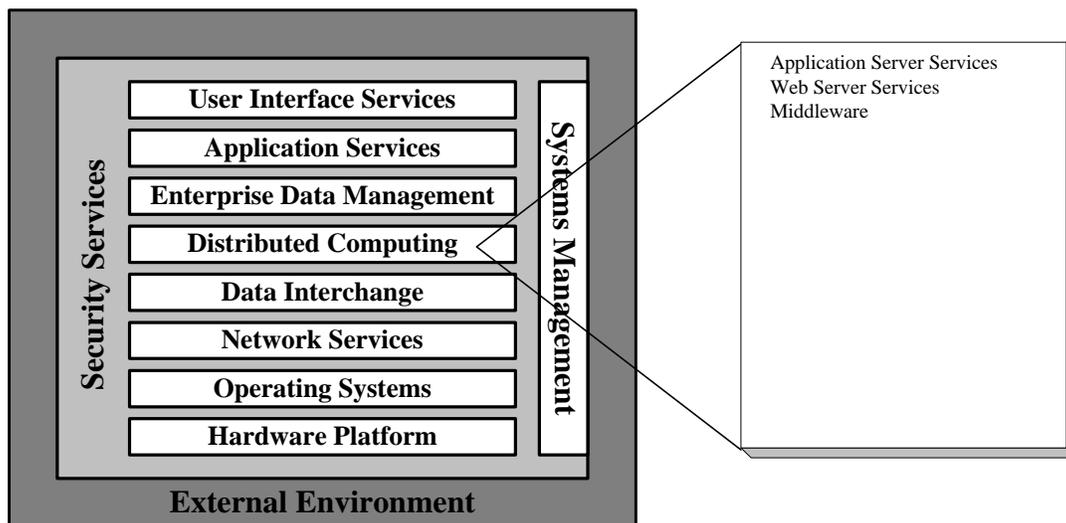


a standard file format for storage may be established.

Rationale: There is no dominant industry standard for imaging services.

4.4 Distributed Computing

Exhibit 4-2: Distributed Computing



Brief Descriptions

Distributed computing services are required to operate similarly across physically dispersed applications. New technologies for the Internet, distributed objects, and security are accelerating the trend toward distributed computing. The combination of computing platforms and communications networks is the key enabling element for modern information systems. The need to support e-business naturally drives the need to interconnect applications. Networks become increasingly important as organizations migrate to distributed processing.

- *Application Servers* provide a deployment platform and execution environment in which application components can take advantage of application server services, such as security functions and transactions, through a web browser. In this environment, individual applications and application components implement business functions with the services provided by the application server. Most application servers provide thread management, database connection pooling, persistence, memory management, logging, naming and directory services, security, application management, transaction support, automatic load balancing, and automatic fail-over support.



- *Web Servers* enable organizations to manage and publish information and deploy network-centric applications over the Internet (public) and intranet (private) environments.
- *Middleware* provides a standard API across hardware and operation system platforms, as well as, networks. Message Oriented Middleware (MOM) performs inter-process messaging that distributes data and control through middleware technology that uses message passing and message queuing to provide peer-to-peer asynchronous communication among programs. Message passing technology has its foundation in a message passing model in which client application programs call an API with as few as four verbs: open connection, send, receive, and close connection. In a distributed message passing model, a client sends a request to the server in the form of a message. The server receives the message and processes the request. The server often creates a new message containing the reply and sends this reply message to the client. Message queuing technology is inherently connectionless. Many message queuing implementations never establish a direct connection between the application client and the application server. With message queuing, however, the sender and receiver can communicate without simultaneous availability, and without the network's direct availability between the sender and receiver. The capability to support discontinuous communication makes message queuing more tolerant of a WAN than other IPC technologies.

Target Standards

Target Standards: Distributed Computing

	FY 2002	FY 2003	FY 2004
Application Server			
	IBM WebSphere Enterprise Edition v3.5.5	IBM WebSphere Enterprise Edition v3.5.5	IBM WebSphere Enterprise Edition v3.5.5
	Oracle Application Server	Oracle Application Server	Oracle Application Server
Web Server			
	IBM IHS Server v1.3.12 (bundled with WebSphere application server)	IBM IHS Server v1.3.12 (bundled with WebSphere application server)	IBM IHS Server v1.3.12 (bundled with WebSphere application server)
	MS IIS	MS IIS	MS IIS
	Netscape Server	Netscape Server	Netscape Server
Middleware			
	MQ Series Server v5.2	MQ Series Server v5.2	MQ Series Server v5.2
	MQ Series Client v5.2	MQ Series Client v5.2	MQ Series Client v5.2
Application Specific			
	TBD	TBD	TBD



Approved Standards

Application Servers – IBM WebSphere Enterprise Edition v3.5.5, Oracle Application Server

Description: SFA application servers will extend SFA’s capabilities by hosting net-centric applications as well as providing application architecture for enabling the development and execution of common services across different business capabilities. The SFA application server will deploy and manage enterprise application components and services; provide secure, web-enabled access to both web-based and legacy application services; and provides an open, standards-based opportunity for reuse of enterprise business logic.

Rationale: The SFA application server will comply with the following standards:

- Java Virtual Machine (JVM) compliant with Java v1.2 or greater;
- Support Enterprise Java Beans (EJB) v1.0 or greater;
- Support Java Server Pages (JSP) v1.0 or greater;
- Support Java Servlet API 2.1;
- Support for Java Database Connectivity (JDBC);
- Support for Java Naming and Directory Interface (JNDI);
- Support for Java Messaging Service (JMS) and Java mail standards;
- Support for MIME.

Web Servers – IBM IHS Server v1.3.12 (bundled with WebSphere application server), MS IIS, Netscape Server

Description: The SFA web server services will provide client communication, communication security, dynamic page services, and application logic. This will allow SFA to handle client requests for HTML pages, process scripts such as Java Server Pages (JSP), and cache Web pages.

Rationale: Web server products must support the SFA COE, including platform support and Internet protocols (HTTP). Standards are:

- Support HTTP v1.0 and HTTPS
- Support JSP v1.0 or greater
- Support Java Servlet API 2.1



- Support SSL
- FIPS 140-1 compliant

Middleware – MQSeries Server v5.2, MQSeries Client v5.2

Description: SFA will have an open and scalable messaging and information infrastructure, which will be used to integrate business processes across different hardware and software platforms. This tool will exchange information among applications across several platforms, such as from Mainframes-OS/390, HP/UX, Sun Solaris, and Windows. SFA will provide an automated solution to integrate software applications across the enterprise, provide rules engine routes for every message to the correct location with table-driven rules bases, and transform data on the fly across DB2 and Oracle application systems.

Rationale: The Message Passing Interface (MPI-2) and the Oxford University Bulk Synchronous Parallel (BSP) model are emerging standards for portable messaging APIs and interoperable messaging protocols. The SFA standard is MPI-2 and BSP.

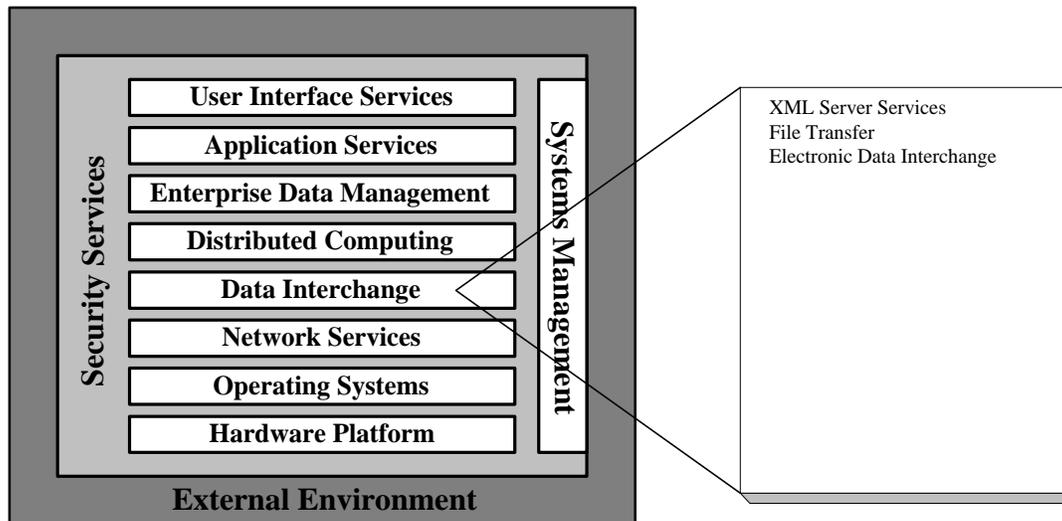
Application Specific Standards – TBD

Description: SFA will have an open and scalable messaging and information infrastructure, which will be used to integrate business processes across different hardware and software platforms. This tool will exchange information among applications across several platforms, such as from Mainframes-OS/390, HP/UX, Sun Solaris, and Windows. SFA will provide an automated solution to integrate software applications across the enterprise, provide rules engine routes for every message to the correct location with table-driven rules bases, and transform data on the fly across DB2 and Oracle application systems.

Rationale: The Message Passing Interface (MPI-2) and the Oxford University Bulk Synchronous Parallel (BSP) model are emerging standards for portable messaging APIs and interoperable messaging protocols. The SFA standard is MPI-2 and BSP.



4.5 Data Interchange



Brief Description

Data interchange services provide specialized support for the exchange of information between applications and the external environment. These services are designed to handle data interchange between applications on the same platform and applications on different platforms. Data interchange services include:

- *XML Servers* provide secure, high-volume data integration between systems. This allows for structured, application-independent and database-independent data transfer between enterprises over the Internet via encrypted XML-formatted documents.
- *File Transfer* services allow users to copy, replicate, or move whole files across a network. The TOG and ISO standards for File Transfer, Access, and Management (FTAM) help provide this service across a heterogeneous network of conforming systems. In addition, File Transfer Protocol (FTP) is an industry-prevalent mechanism that is found with most TCP/IP implementations. Although FTAM and FTP are specialized means of transferring files, it is also possible to use the e-mail system for transporting files. A standard called Multipurpose Internet Mail Extensions (MIME), which has emerged from the Internet mail protocol (SMTP), permits various file types to be transferred as mail attachments. All mail systems have limits on the size of files they can transfer; some are as small as 32 KB.
- *Electronic Data Interchange (EDI)* is the intra- and inter-organizational, computer-to-computer exchange of information in a standard format without human intervention. The idea behind EDI is to take what has been a manually prepared form, a form from a business application, or information, translate that data into a standard electronic format, and transmit it. At the receiving end, the standard format is “untranslated” into a



format that can be read by the recipient’s application. Hence, output from one application becomes input to another through the computer-to-computer exchange of information. The benefits of EDI are:

Cost reductions from eliminating paper document handling and faster electronic document transmission.

Improvements in overall quality through better record keeping, fewer errors in data, reduced processing time, less reliance on human interpretation of data, and minimized unproductive time.

Better information for management decision making. EDI provides accurate information and audit trails of transactions, enabling businesses to identify areas offering the greatest potential for efficiency improvement or cost reduction.

Optimum benefits are achieved through reengineering business processes and utilizing EDI and other electronic commerce technologies as enablers.

Target Standards

Target Standards: Data Interchange

	FY 2002	FY 2003	FY 2004
XML Server	Innovision XML Server	Innovision XML Server	Innovision XML Server
File Transfer	FTP, HTTP, SMTP (MIME), FTAM, and SNA	FTP, HTTP, SMTP (MIME), FTAM, and SNA	FTP, HTTP, SMTP (MIME), FTAM, and SNA
Electronic Data Interchange	XML (May 5 W3C XML Schema Recommendation)	XML (May 5 W3C XML Schema Recommendation)	XML (May 5 W3C XML Schema Recommendation)

Approved Standards

XML Server – Innovision XML Server

Description: The SFA XML server will provide data security services, XML parsing services, and XML processing services. This will allow SFA to send XML-formatted data securely over the Internet using HTTP-S encryption; read XML-tagged documents and interpret the self-described data structure of the data elements; and store XML-parsed data and associated structure in memory—using open standards such as Document Object Model



(DOM)—for use by application or database.

Rationale: XML server products must support the application of XML throughout the enterprise using SFA-defined security services and provide for Java-based access to DOM-compliant data structures.

File Transfer – FTP, HTTP, SMTP (MIME), FTAM, and SNA

Description: Current tools and methods assume that any encryption requirements are handled before and after file transfers. Future implementations will likely integrate encryption support. SFA will select file transfer systems that conform to widely accepted industry standards and promote interoperability between the defined platforms. The use of e-mail methods for file transfer will be limited to small files and driven by specific business requirements that cannot be met by other standard technologies.

Rationale: SFA standards for file transfer are FTP, HTTP, SMTP (MIME), FTAM, and SNA. SMTP will be the SFA standard for mail systems.

Electronic Data Interchange – XML

Description: SFA will develop new intra- and inter-organizational data interchange using XML or the related W3C standards (e.g., X-Schema, XQL, XLink). Moreover, as part of the financial industry, SFA will participate in and adopt those data interchange standards generally accepted by partners and customers (e.g., Rosetta-Net).

These transactions are similar to other X12 transaction sets except for a few differences. One difference is that the interactive transactions are wrapped in variable-length EDIFACT headers and trailers instead of in the longer fixed-length X12 envelope. Another difference is that segments are very concise, with limitations on repetitions of groups of segments. The number of mandatory segments and data elements has also been kept to a minimum.

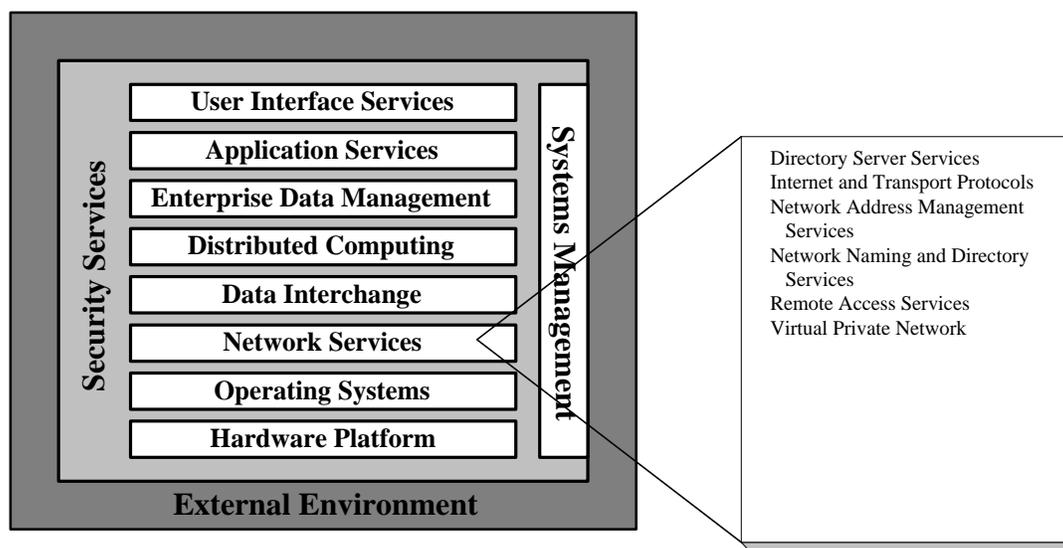
XML is a new technology based on the Standard Generalized Markup Language (SGML) from which HTML is also derived. XML allows one to indicate the values of data within a document, such as `<price>9.99</price>`. XML may be the means to bridge EDI into Internet electronic commerce, by making the existing EDI knowledge base more palatable to the Internet electronic commerce developers. Because of this,



CommerceNet Consortium, XML/EDI Group, and ANSI X12 have entered into a joint project to investigate how to translate ANSI ASC X12 data elements, segments, and transactions into XML.

Rationale: SFA will use EDI with ANSI X12 standards and XML for continued data distribution with schools, guarantor agencies, and other business partners.

4.6 Network Services



Brief Descriptions

Network services are provided to support distributed applications requiring data access and applications interoperability in heterogeneous or homogeneous networked environments. Network services consist of both an interface and an underlying protocol and include the following:

- *Directory Servers* provide a central data repository that simplifies communication and the sharing of resources. It allows diverse applications, machines, and users (both inside and outside the enterprise) to access the same information and services, which simplifies tasks such as e-mail naming and addressing, maintenance of computing environments, and user authentication and authorization.
- *Internet and Transport Protocols* delivers end-to-end services across physically and logically diverse data networks. Physically diverse networks range from LANs in separate departments



to enterprise networks owned by separate companies. Logically diverse networks are defined by the different architectures or products used in their construction.

- *Network Address Management Services* provides each network element and user an identity that is used by other elements to reference its location on the network. For most networks, some form of name and address is an integral part of operation. Naming schema and addressing schema are unrelated. A name is used to identify an object; an address provides the its locate on the network. When an object is relocated on the network, its network address changes; however, the object name may remain the same.
- *Network Naming and Directory Services* are needed to locate resources on the network. These services provide the means for identifying and retrieving information about objects on the network. An object is a specific resource on the network such as a computer, application, file, electronic mailbox, printer, or router. Information that can be retrieved about an object varies according to the object and the name or directory service providing the information. Naming and directory services are related in the functions they provide, but distinct differences still exist. A naming service locates and retrieves information about an object solely by the name of the object.
- *Remote Access* provides secure distributed computing resources into the field. Remote clients have two methods of accessing local enterprise network resources: over the Public Switched Telephone Network (PSTN) or through “tunneling” through the Internet. Remote access allows a remote PC to dial into a central server and operate exactly as if it were directly attached to the LAN. Network protocols are transferred transparently across the connection, allowing security and authentication. Remote Node applications scale well, since the connection is largely transparent to the user and multiple calls can be consolidated onto a single ISDN and/or modem server for LAN access.
- *Virtual Private Networks (VPN)* are private, secured networks that exists within a public network and are shared by many private users. The technologies used in creating VPNs include X.25, switched 56, frame relay, and ATM. The main drivers of Internet-based VPNs are the desire to replace current high-cost wide-area or enterprise-level networking solutions and providing high-speed access to corporate resources for remote and mobile employees, as well as strategic partners. Internet VPNs work by creating a tunnel through the public Internet through which encrypted information is transmitted. Internet VPNs providing data encryption and, in some cases, manage the stability and reliability of the network connection. Corporate VPNs over the internet are not always suitable. Internet VPNs are not optimal as the corporate backbone network, for the transmission of streaming data or multimedia, or when a high level of data security is required. Internet VPNs are well suited for thin-client applications, such as web browsers, and intelligent message-queuing applications, such as e-mail, that minimize data transmissions and can tolerate disruptions and delays.



Target Standards

Target Standards: Network Services

	FY 2002	FY 2003	FY 2004
Directory Servers			
	Netscape Directory Server	Netscape Directory Server	Netscape Directory Server
Internet and Transfer Protocols			
	TCP/IP	TCP/IP	TCP/IP
	SNA	SNA	
		VOIP	VOIP
Network Address Management			
	Static IP	Static IP	Static IP
	DHCP	DHCP	DHCP
Network Naming and Directory Services			
	DNS	DNS	DNS
Remote Access Services			
	Cisco Secure RADIUS	Cisco Secure RADIUS	Cisco Secure RADIUS
	Citrix	Citrix	Citrix
Virtual Private Network			
	CheckPoint VPN-1	CheckPoint VPN-1	CheckPoint VPN-1

Approved Standards

Directory Servers – Netscape Directory Server

Description: The SFA directory server will provide name and domain services, including single sign-on capability, common data store for personalization preferences, and common source of user authentication and privileges.

Rationale: LDAP is an industry standard for directory services.

Internet and transport protocols – TCP/IP

Description: SFA is committed to migrating to a single managed, secure, wide area data network. SFA will migrate to the TCP/IP network protocol and increasingly restrict the use of SNA traffic. Voice Over Internet Protocol (VOIP) is a group of Internet telephony products redefining the details for digitally delivering real-time voice communications over the Internet and



other IP networks. As the technology matures, SFA will use VOIP for mobile Internet access.

Rationale: TCP/IP, a strategic step toward interoperability, uses a common network infrastructure. TCP is the transport (OSI Level 4) layer, and IP is the network (OSI Level 3) layer.

The VOIP standard derives from the VOIP Forum recommendation that members standardize on the ITU's G.723.1 audio codec, thus providing a path toward interoperable Internet telephony equipment from multiple vendors. The G.723.1 codec is also included in the ITU's H.323 standard, an umbrella standard that establishes how audio, video, and data communications take place over IP networks.

Network Address Management – DHCP, Static IP

Description: SFA employs DHCP, which is currently administered by the Department of Education, as its standard network address management service. An assessment of the Infrastructure Architecture will determine if SFA's current DHCP implementation will scale to support native TCP/IP on all desktops. While DHCP is not intended to support mobile users, it is valuable in supporting laptop plug-in at remote locations. DHCP actually assigns a new IP address to the end system, so the DNS database must change (which requires some settling time) before full service catches up.

A static IP address is assigned to server and specialized development computers.

Rationale: DHCP is defined in IETF RFC 2200, and NAT standards currently have IETF recommended RFC status.

Network Naming and Directory Services – DNS

Description: SFA will utilize a consistent, globally unique naming and addressing scheme. This naming scheme is required for the objects being stored in both naming and directory systems. The names of the objects will be logical and meaningful to the system users and other applications. A name should conform to the following three principles:

- Alphanumeric format that clearly conveys the built-in meaning



- Unique within its domain
- Not overly encoded or in hexadecimal format, except for security purposes

Rationale: The SFA standard for naming services is DNS. Currently, DNS services are administered by the Department of Education. SFA will consider implementation of an integrated, hierarchical directory service based on the LDAP and X.500 directory services standards in the next iteration of the infrastructure architecture. X.500 is the leading standard for directory services. The X.509 standard (the ITU-recommended standard for digital certificates) should be fully supported in any selection of an X.500 directory system.

Remote Access –Cisco Secure RADIUS, Citrix

Description: In most common implementations, users connect their personal computers to the Internet with high-speed modems. Using a modem to connect to a terminal server, with point-to-point protocol (PPP) there is a more direct and flexible connection. Many of the functions accessed by dialing up a terminal server and running them on a remote host (such as a UNIX shell account) can also be run from a personal computer. For instance, PPP allows the use of e-mail and web browser programs that take advantage of a workstation's graphics capabilities, graphical user interface, and other special features.

Rationale: The SFA standard will be PPP, which will be used for connecting to networks over standard serial (telephone) lines.

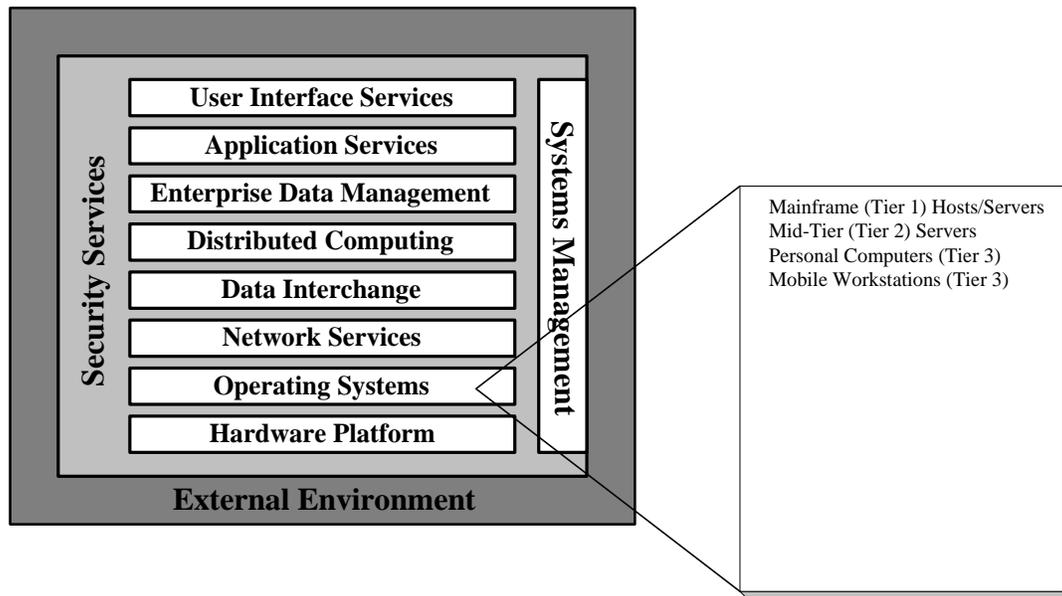
Virtual Private Network – CheckPoint VPN-1

Description: SFA will use VPN software capable of encrypting data for tunneling through network connections through the public internet.

Rationale: No published industry standard identified.



4.7 Operating Systems



Brief Description

Operating system services are responsible for the management of platform resources, including the processor, memory, files, and input and output. They generally shield applications from the implementation details of the machine. Operating system services include:

Kernel operations, which provide low-level services necessary to create and manage processes and threads of execution, execute programs, define and communicate asynchronous events, define and process system clock operations, implement security features, manage files and directories, and control input/output processing to and from peripheral devices.

Command interpreter and utility services, which include mechanisms for services at the operator level, such as comparing, printing, and displaying file contents, editing files, searching patterns, evaluating expressions, logging messages, moving files between directories, sorting data, executing command scripts, local print spooling, scheduling signal execution processes, and accessing environment information.

Batch processing services, which support the capability to queue work (jobs) and manage the sequencing of processing based on job control commands and lists of data.



File and directory synchronization services, which allow local and remote copies of files and directories to be made identical. Synchronization services are usually used to update files after periods of off line working on a portable system.

The operating system platforms employed by SFA are provide the following capabilities:

- *Mainframe (Tier 1) Hosts/Servers* operating system provides one host which communicates with multiple clients. Users can explore existing corporate data to locate patterns and structures that will provide answers to real-world business questions or new business opportunities. A system with DB2 will provide the capability for handling large databases as a single image.
- *Mid-Tier* operating system services provide the basic environment for running applications. (See the discussion on personal computer operating systems.)
- *Personal Computer (Tier 3)* operating systems using Intel's microprocessors running Microsoft NT Workstation are also being used in high-end computing applications such as application development, multimedia, and decision support data analysis presentation. NT Workstation offers the same user interface and similar user services as Windows, which is more commonly used in general office automation environments today. Both of these operating systems can run on the same hardware platforms, enhancing the ability to combine the right operating system technology with the correct price and performance hardware technology to deliver high-function personal computing to end users. This approach allows performance upgrades to be accomplished more easily during the end user application life cycle.
- *Mobile Workstations (Tier 3)* operating system services provide the basic environment for running applications. (See the discussion on personal computer operating systems in Section 4.7.3.)

Target Standards

Target Standards: Operating Systems

	FY 2002	FY 2003	FY 2004
Mainframe (Tier 1) Hosts/Servers			
	OS/390	OS/390	OS/390
	CICS	CICS	CICS
Mid Tier (Tier 2) Servers			
	HP/UX v11.0	HP/UX v11.0	HP/UX v11.0
	Windows NT	Windows NT	Windows NT
	Windows 2000	Windows 2000	Windows 2000
	Sun Solaris v2.6	Sun Solaris v2.6	Sun Solaris v2.6



Personal Computers (Tier 3)

Microsoft Windows 98			
Microsoft Windows NT Professional	Microsoft Windows 2000	Microsoft Windows 2000	Microsoft Windows

Mobile Computers (Tier 3)

Microsoft Windows 98	Microsoft Windows 2000	Microsoft Windows 2000	Microsoft Windows
----------------------	------------------------	------------------------	-------------------

Approved Standards

Mainframe (Tier 1) Hosts/Servers – OS/390, CICS

Description: The system will provide technology to exploit data warehousing, data mining, and decision support disciplines. The host/server operating system will support current legacy mainframe applications and newly selected COTS applications. The SFA standard for the mainframe operating system is the OS/390 configuration. This OS/390 operating system currently resides on all SFA mainframe systems. SFA uses Parallel Sysplex technology configuration.

Rationale: SFA will use large-scale servers and enterprise computers with operating systems and hardware components that comply with IEEE’s POSIX and Unix95 specifications.

Mid-Tier (Tier 2) Servers – HP/UX v11.0, Windows NT, Windows 2000, Sun Solaris v2.6

Description: The mid-tier operating systems are function-specific with targets as indicated below:

Target Operating System	Function
Windows NT	Application Services Database Services
HP/UNIX	Oracle Platforms Oracle Financials Internet
Sun Solaris	ITA



Rationale: Compliance with XPG 4.2 and POSIX standards allows for increased interoperability of hardware components and facilitates application portability. The capability to easily upgrade processor performance or to add additional processors, disk storage, and communications support extends the life of the platform and enhances the return on investment. Where the NT server meets projected growth requirements, it is an acceptable operating system to use; however, UNIX will continue to offer better scalability for the next few years.

Personal Computers (Tier 3) – Microsoft Windows 2000

Description: The operating system must ensure compatibility and the sharing of data with other personal computer operating systems within SFA's environment and comply with POSIX standard interfaces for long-term usability. SFA has committed to the Microsoft Office and Windows operating system family as a means to establishing a common desktop environment.

Rationale: The personal computer operating system will comply with the SFA Desktop COE and support SFA's standard set of productivity tools. The SFA standard product selection is Microsoft Office 2000 and Windows 2000.

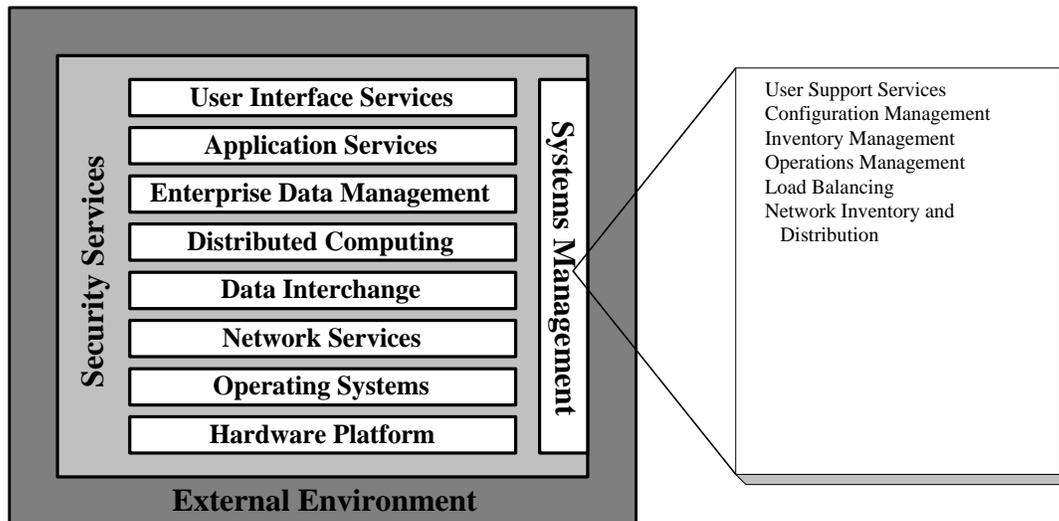
Mobile Computers (Tier 3) – Microsoft Windows 2000

Description: The mobile workstation operating system must ensure compatibility and the sharing of data with other operating systems within SFA's environment and comply with POSIX standard interfaces for long-term usability. SFA has committed to the Microsoft Windows operating system family for a preponderance of business applications on mobile workstations.

Rationale: The mobile workstation operating system will comply with the SFA Desktop COE and support SFA's standard set of productivity tools. The SFA standard product selection is Microsoft Windows 2000.



4.8 Systems Management



Brief Descriptions

Systems management refers to information technology activities that do not relate to application execution or development. It includes everything from the daily operations, management, and service of information system to long-range planning for future business needs. Systems management comprises the processes, procedures, tools, and techniques that are implemented through personnel and automation to ensure the cost-effective operation of information systems. The procedures and tools ensure proper planning, configuration, and problem handling of IT resources. Systems management includes the following:

- *User Support Services* collects requirements from and coordinates with the users of services. User requirements include change requests, requests for additional service, requests for new services, and problem requests. The user help desk interface function tracks requests and problems until resolution is achieved and provides feedback to the users.
- *Configuration Management (CM)* enables maintaining, adding, and updating the relationships among components and the status of components themselves during system/network operation. End user service is provided by the configuration of the various system and network components into an integrated and cohesive function. CM includes the automatic capture and storage of program component relationships and maintenance of the history of those relationships and transformations. It is becoming increasingly difficult to maintain, control, and manage software, and software is becoming more complex and pervasive in the delivery of IT services to users. For those reasons, software configuration management (SCM) has become a major component of the total software maturity process. SCM addresses



all aspects of CM by managing software and its changes with complete security, integrity, and audit capability for the life of the software.

- *Inventory Management* provides a repository of accurate and timely data about managed resources. Inventories are used to track expected occurrences of the resources against the actual existence of the resources. Inventories may also include various reference information such as location, owner, or vendor contact. SFA should maintain an accurate inventory of the major systems based on the 1997 lawsuit *Public Citizen v. Raines*.
- *Operations Management* supports and controls the current, implemented infrastructure. The primary tasks of operations include the following:

Fault management—Fault identification, isolation, recovery, resolution, and message filtering.

Performance management—System and network data collection and logging. This is comprised of two broad functional categories, monitoring and controlling. Monitoring is the function that tracks activities on the system/network (i.e., its performance). The controlling function enables performance management to make adjustments to improve system/network performance.

Change control—Change coordination, approval, and implementation.

Accounting management activities—Ability to determine by cost centers, or even individual project accounts, the use of systems/network services. Additionally, the systems/network manager needs the ability to track the use of system/network resources by component or component class (type).

Hierarchical storage management—Dynamic placement of data across various storage technologies such as memory, disks, and tapes, based on usage and retention parameters.

Routine activities—Scheduling and common services such as backups and preventive maintenance.

- *Load Balancing* has three major components. (1) Load balancing software, which distributes web site traffic between servers, leading to better response times for online users. (2) Caching proxy server, which captures web site images that can be retrieved locally in subsequent requests, reducing network traffic. (3) Enterprise file system, which provides content replication.
- *Network Inventory and Distribution Services* provide a mechanism for centrally distributing and modifying software across distributed environments. For inventory, the system automatically scans for and collects hardware and software configuration information from computer systems in the enterprise.



Target Standards

Target Standards: System Management

	FY 2002	FY 2003	FY 2004
User Support Services			
	TBD	TBD	TBD
Configuration Management			
	Computer Associates Harvester Change Manager (Mid-Tier)	Computer Associates Harvester Change Manager (Mid-Tier)	Computer Associates Harvester Change Manager (Mid-Tier)
	Computer Associates Endeavor (Mainframe)	Computer Associates Endeavor (Mainframe)	Computer Associates Endeavor (Mainframe)
	Rational ClearCase v4.1 (Non-mainframe)	Rational ClearCase v4.1 (Non-mainframe)	Rational ClearCase v4.1 (Non-mainframe)
	Rational ClearQuest 2001 v4.0 (Mid-Tier)	Rational ClearQuest 2001 v4.0 (Mid-Tier)	Rational ClearQuest 2001 v4.0 (Mid-Tier)
Inventory Management			
	Self-built solution	Self-built solution	Self-built solution
Operations Management			
	Computer Associates CA-7 (Mainframe)	Computer Associates CA-7 (Mainframe)	Computer Associates CA-7 (Mainframe)
	BMC Control D (Printing)	BMC Control D (Printing)	BMC Control D (Printing)
	BMC Control M/R (Mainframe)	BMC Control M/R (Mainframe)	BMC Control M/R (Mainframe)
	Hewlett Packard OpenView (Network Monitor)	Hewlett Packard OpenView (Network Monitor)	Hewlett Packard OpenView (Mid-tier)
Load Balancing			
	IBM WebSphere Performance Pack v3.0	IBM WebSphere Performance Pack v3.0	IBM WebSphere Performance Pack v3.0
	Cisco Director	Cisco Director	Cisco Director
Network Inventory and Distribution Services			
	Microsoft Software Management System (SMS)	Microsoft Software Management System (SMS)	Microsoft Software Management System (SMS)
	Lotus Notes	Lotus Notes	Lotus Notes
	Candle Management	Candle Management	Candle Management



Approved Standards

User Support Services – TBD

Description: To be determined

Rationale: No published industry standard identified.

Configuration Management – Computer Associates Harvest Change Manager (Mainframe), Computer Associates Endeavor (Mainframe), Rational ClearCase v4.1 (Non-Mainframe), Rational ClearQuest 2001 v4.1

Description: To be determined

Rationale: No published industry standard identified.

Inventory Management – Self-built solutions

Description: There are solutions that have been developed by both the Department of Education and SFA currently being used.

Rationale: To be determined.

Operations Management – Computer Associates CA-7 (Mainframe), BMC Control D (Printing), BMC Control M/R (Mainframe), Hewlett-Packard OpenView (Network Monitor)

Description: SFA will use operations management solutions that will ensure that individual distributed systems and mainframe technologies work in harmony to create a positive automated environment.

Rationale: The SFA standard will be SNMP (Simple Network Management Protocol) as a generic network management tool. An SNMP message is sent to and from a device to gather information or configure the device.



Load Balancing – IBM WebSphere Performance Pack, Cisco Director v3.0

Description: Load balancing will performs the following features:

- Rules-based routing to detect and react to sudden increases in activity
- Load balancing based on the content of HTTP requests at an application level
- Use of a public key/private key pair to control communication and make remote administration more secure
- Transparent load balancing and a mechanism to catch and log misdirected or malicious packets
- Proxy sharing of cached content
- Garbage collection based on user-defined usage specifications or at user-specified times
- Remote administration using the security features provided by SSL
- Reverse proxy to permit more concurrent connections and to accelerate Web server performance

Rationale: No published industry standard identified.

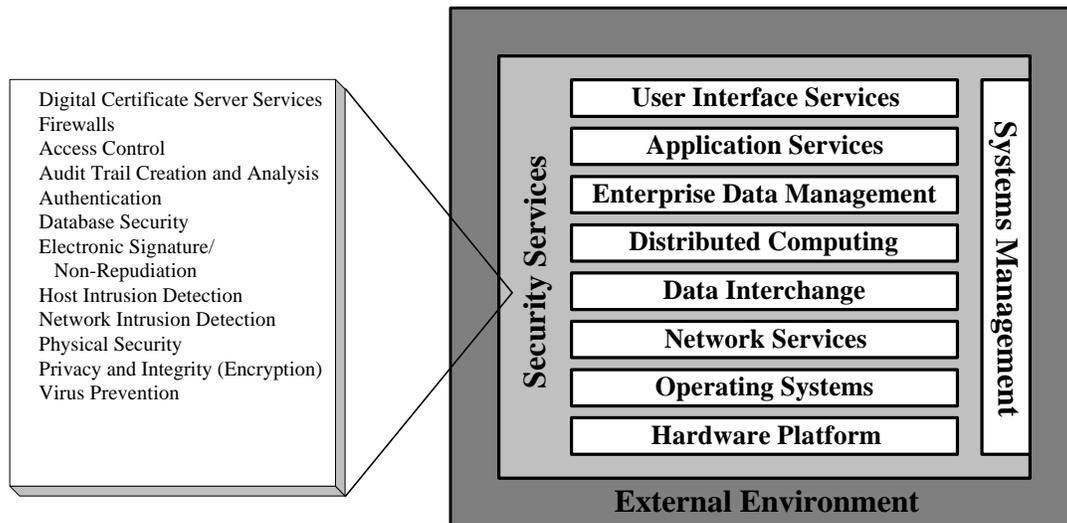
Network Inventory and Distribution Services – Microsoft Software Management System (SMS), Lotus Notes, Candle Management

Description: To be determined

Rationale: No published industry standard identified.



4.9 Security Services



Brief Description

Office of Management and Budget (OMB) Circular A-130 Appendix III requires that all agencies implement and maintain a security program that provides “adequate security” for information, processes, and systems. Adequate security is defined as security controls commensurate with the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to or modification of information stored or flowing through these systems. Security controls may be physical, management, personnel, operational, or technical, and implemented by hardware or software security.

An *Office of Student Financial Assistance Guide to Information Security and Privacy* has been created by SFA. This guide provides a view of the existing Department of Education Information Security Policy and how it relates to SFA. It also outlines procedures that should be used to reduce risk and ensure that SFA systems are available to SFA customer and partners in a time manner.

The *Security Architecture* and *SFA Information Security General Minimum Security Baseline Standards* security documents are current under development by SFA Modernization Partners. These documents will detail security architecture and standards for SFA. A Minimum Security Baseline (MSB) will be used as the standard for implementing a minimum level of security on all SFA information systems. The following section outlines several technical security policy and standards that should be used to protect SFA information systems, data, networks, and applications.



- *Digital Certificate Servers* provide a specially coded object that uniquely identifies a site. Object contains the site's public key for encryption and the site's identification information such as organization name, expiration date, and a digital signature of the issuer. It allows verification of the claim that a specific public key does, in fact, belong to a specific individual. These certificates are used by the settings within browsers and firewalls to either permit or restrict users from accessing or downloading components to their machines. Certificate management and access provide for primary components of information security, including authentication, authorization, encryption, and non-repudiation.
- *Firewall* services protect sensitive information and resources that are attached to a network from unauthorized access. A firewall is a system that prevents the hazards of the internet from extending to internal network. It enforces a boundary between two or more networks. There are two types of firewall policies: deny any service (or packet) not explicitly permitted or permit any service (or packet) not explicitly denied. In general the various firewall security mechanisms address themselves to specific layers in the OSI 7-level network model. Several mechanisms can be combined into a comprehensive firewall system, but the mechanisms should be chosen and coordinated so that they do not interfere with each other. A variety of firewall implementations may be required at various levels within the network. Each type of policy and type of firewall has its advantages and disadvantages. Firewalls should encompass two components: packet filters and proxy services. Packet filters provide network-level security. These are protocol-based services that check the address portion of data packets to determine the desired destination and intent. Administrators can block certain combinations that are categorized as unauthorized. Proxy services provide application-level security. Proxy services shield or screen the server address, thus preventing outsiders from knowing the specific addresses of servers within the private network (and later targeting them).
- *Access Control* is achieved by a combination of physical and logical access. Logical access control mechanisms permit access to a machine, a file, or an application only after the client (e.g., employee, machine, application) establishes its identity and authentication. Typically there are several layers of access control, e.g., physical control for access to the system, authorization for access to an account, and access control lists for access to individual applications. In the n-tier client/server computing environment, access control may be practiced at every tier.
- *Audit Trails Creation and Analysis* are used to detect and deter penetration of a computer system and to reveal usage that identifies misuse. At the discretion of the auditor, audit trails may be limited to specific events or may encompass all the activities on a system. Audit trails may be used as either a support for regular system operations or a kind of insurance policy or as both of these. As insurance, audit trails are maintained but are not used unless needed, such as after a system outage. As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications. The audit trails have four important security objectives:

Individual accountability



Reconstruction of events

Intrusion detection

Problem analysis

- *Authentication* is the means of proving the identity of a subject to system, networks, and applications. Entering an assigned value (USERID) performs identification and authentication is performed by entering a value or by physical means. The authentication methods should be totally under the control of the individual. The mechanism for authentication of a user generally depends on one or more of the following: something the user knows (a password or encryption key), something the user possesses (a key, token, or magnetic security badge), or some physical characteristic (biometrics) of the user such as a fingerprint. Authentication mechanisms employing tokens or biometrics provide a significantly higher level of security than passwords and are referred to as advanced or strong authentication mechanisms. However, when sending information over remote network connections, particularly over public networks without security procedures, it is possible to impersonate users and other entities in a public network.
- *Database Security Services* contribute to the protection of information, data, and resources in open systems in accordance with applicable SFA information domain and information system security policies. An information domain is a set of users, their information objects, and a security policy. An information domain security policy is the statement of the criteria for membership in an information domain and the required protection of the information objects. These information domains are not bounded by systems or even networks of systems. The provision of DBMS security services includes the following activities:
 - Data security policy management
 - Data security service management
 - Data security mechanism management
 - Data security mechanism support management
- *Electronic Signatures/Non-repudiation* provides the means to prove that a digital transaction actually occurred, i.e., some form of electronic receipt. Digital signatures and file integrity checks use strong encryption to protect data integrity and guarantee data authenticity with a reasonable degree of assurance. SFA may have a need for strong non-repudiation requirements so those individuals can be held accountable for messages they send.
- *Host Intrusion Detection* focuses on events occurring within a system as reported by the various logs in a system, for example, repeated failed logins, attempts to access or modify certain files, or changes in usage patterns. Firewalls will reduce but not entirely eliminate the risk of unauthorized external access to SFA networks and systems. Intrusion detection



systems, the digital equivalent of burglar alarms, and alarm messages they produce may be linked into the systems management process.

- *Network Intrusion Detection* focuses on examining packets on the network for known attack patterns. The detection agent functions by looking for actual attempts to exploit the vulnerabilities of the systems and the networks.
- *Physical Security* is an effective means to provide security within individual sites in the SFA computer network. While not practical for security of small remote sites and mobile computers (e.g., laptops), physically restricting access to machines in central locations under SFA control is an important part of overall systems security. Physical security policies may be enhanced through the deployment of appropriate monitoring systems.
- *Encryption* provides protection for information stored and routed on computer networks managed by SFA meeting privacy and integrity requirements. Some applications include the transmission of information, interception or alteration of which should be protected. Such applications include remote terminal access, bulk transfer of data extracted from legacy systems and online database access. Firewalls alone cannot protect such data outside the local perimeter. Currently many forms of encryption software are available. They are based on various standards (e.g., Secure Telnet (Stel), the Data Encryption Standard (DES), Rivest, Shamir, Adleman (RSA), etc.). The recommendation implies that any standards-based encryption is better than allowing the transmission of clear text across wide-area networks.
- *Virus Protection* provides virus prevention and detection in a variety of network environments. Many forms of computer information can contain harmful content including viruses, macro viruses, and Trojan horse programs. These “malicious programs” can be transmitted across a network in a number of ways including SMTP e-mail attachments, FTP file downloads, and Java applets. Incoming data can be checked for harmful content at the public Internet work boundary. Passive virus protection should be implemented throughout the network environment. Products chosen should protect against the widest possible array of viruses, and should be compatible with the SFA’s architectures.

Target Standards

Target Standards: Security Services

	FY 2002	FY 2003	FY 2004
Digital Certificate Server Services			
	Netscape Certificate Server	Netscape Certificate Server	Netscape Certificate Server
Firewall Services			
	CheckPoint Firewall-1	CheckPoint Firewall-1	CheckPoint Firewall-1
Access Control			
	RACF (Mainframe)	RACF (Mainframe)	RACF (Mainframe)
	BMC Control SA	BMC Control SA	BMC Control SA



Audit Trail Creation			
	System Log File	System Log File	System Log File
Authentication			
	RACF (Mainframe)	RACF (Mainframe)	RACF (Mainframe)
	BMC Control SA (Mainframe)	BMC Control SA (Mainframe)	BMC Control SA (Mainframe)
	TBD (Mid-tier)	TBD (Mid-tier)	TBD (Mid-tier)
Database Security Services			
	RACF (Mainframe)	RACF (Mainframe)	RACF (Mainframe)
	Top Secret (Mainframe)		
	TBD (Mid-tier)	TBD (Mid-tier)	TBD (Mid-tier)
Electronic Signatures/Non-repudiation			
	TBD		
Host Intrusion Detection			
	Tripwire (Windows NT)	TBD	TBD
	Tripwire (Sun Solaris)	TBD	TBD
	Tripwire (HP-UX)	TBD	TBD
Network Intrusion Detection			
	RealSecure	RealSecure	RealSecure
Physical Security			
	See OMB A130	See OMB A130	See OMB A130
Encryption			
	Secure Socket Layer	Secure Socket Layer	Secure Socket Layer
	BSAFE	BSAFE	BSAFE
	Triple DES	Triple DES	AES
Virus Protection (Desktop)			
	McAfee	McAfee	McAfee
	Norton Antivirus	Norton Antivirus	Norton Antivirus

Approved Standards

Digital Certificate Server Services – Netscape Certificate Server

Description: The SFA digital certificate server will provide authentication, issuance, and revocation services, including the capability for future digital signature administration. Digital certificate server services will be part of the overall, comprehensive SFA security procedures.

SFA digital certificate server services will be capable of handling large numbers of certificates and will provide capabilities that work across all browsers and servers. Authentication services will verify that the presenter



of a set of credentials matches the owner on record. Issuance services will generate public/private keypairs. Revocation services will maintain a list of certificates that have been revoked and be able to share that list with other certificate servers.

Rationale: The X.509 digital certificate involves the ITU-T Recommendation X.509 [CCI88c], which specifies the authentication service for X.500 directories as well as the widely adopted X.509 certificate syntax.

Firewall Services – CheckPoint Firewall-1

Description: SFA firewalls will provide policy-driven restrictions on network connections, protocols, and data formats, including authentication-driven restrictions on data exchanges by applications and individuals. This will include the use of a hybrid firewall, which will provide both network-level and application-level security, located between the back-end servers and the certificate server.

All communication between the SFA enterprise and the public network will pass through the SFA network firewall. The design philosophy of the SFA's Internet connectivity is to provide unrestricted outbound access to Internet resources with inbound access limited by the firewall rules. This philosophy provides the maximum protection for servers/workstations inside of EDNet while allowing EDNet users sufficient accessibility to Internet resources to complete their mission.

The following firewall directives will apply to all existing and future firewall implementations:

- All interconnections to the SFA private intranet from other networks must use the TCP/IP protocol. All protocols/services not specifically noted in this document are prohibited except by specific approval from SFA Security.
- All existing and future untrusted networks connecting to the SFA private intranet require an SFA Security-certified firewall implementation.
- Only SFA Security-approved personnel are permitted to perform any firewall administration.
- All firewall interconnections to the SFA private intranet, whether existing or proposed, must be documented and the documentation must be provided to SFA Security.



Rationale: ICSA standards body and relevant standards are identified in the Department of Education Security Policy and the evolving SFA Security Architecture.

Access Control – RACF (Mainframe), Top Secret (Mainframe), BMC Control SA

Description: Access authorization should be based in part, on the responsibilities and functions performed. This should include application and well as individual system access. Security profiles can be defined with specific access requirements. These profiles can contain sufficient information to determine which networks, systems, applications and files that one is permitted to access. Access control lists can detail individual entities or descriptions of specific profiles. Access control mechanisms must manage the access control attributes of subjects to objects and ensure that they are protected. Access control mechanisms must manage who should grant access to objects and to who access might be granted. Only an authorized person can grant access to an object.

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving SFA Security Architecture.

Audit Trail Creation – System Log File

Description: When a security-relevant event occurs, the security audit service must generate an audit event that can be recorded, reported, archived, and analyzed. Use security products that generate an incorruptible audit record and support the analysis and dissemination of records. Such products must provide the ability to determine which events are recorded and reported within a security domain.

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving SFA Security Architecture.

Authentication – RACF (Mainframe) BMC Control SA (Mainframe), TBD (Mid-tier)

Description: Authentication will ensure that every subject or object using the system is identified. Identification will be enforced for both login sessions established through direct connected devices such as desktop workstations, and through remote devices, such as dial-up connections. Typically, an



operating system's password authentication capabilities will be used. Other authentication devices such as smart cards, biometrics-measuring devices (fingerprints or retina image) are challenge response methods. No authentication data should be available to unauthorized subjects or objects. Authentication information such as password should never be stored in clear text.

SFA authentication will also encompass the following areas:

- Warning to unauthorized user that the system is security aware
- Authentication of the user
- Password should be at eight with digits and characters
- Periodic changing of password
- No reuse of previous password
- Time of session when left unattended
- Information displayed on entry, about previous successful and unsuccessful login attempts
- Authentication suspended after three fail attempts

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving SFA Security Architecture.

Database Security Services – RACF (Mainframe), Top Secret (Mainframe), TBD (Mid-Tier)

Description: The database maintains the user, user groups and controls permissions for all database resources – tables, views, fields, and other database objects. Most databases have their own list of users and groups. Database controls user accesses rights at each level. Own level access is usually controlled through views. PEPS database environment is Oracle, which maintains users and groups. Oracle controls access to rows based upon database views.

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving SFA Security Architecture.



Electronic Signatures/Non-repudiation – TBD

Description: To be determined.

Rationale: To be determined.

Host Intrusion Detection – Tripwire

Description: SFA host intrusion detection will be widely deployed and will be a trusted security/administration product. The tools will alert SFA the moment a protected file has been altered or tampered whether it is caused by a predatory hacker, a disgruntled employee, or simply an inadvertent slip-up. It will identify what was changed and provide means to undo any damage. SFA has selected Tripwire as the standard software for intrusion detection.

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving SFA Security Architecture.

Network Intrusion Detection – RealSecure

Description: To be determined.

Rationale: No published industry standard identified.

Physical Security – See OMB A130

Description: The Department of Education has published policy on the physical security of systems. This will be adopted by SFA until an SFA-specific policy is developed.

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving SFA Security Architecture.

Encryption – Secure Socket Layer, BSAFE, Triple DES

Description: Data Encryption Standard (DES) or RSA algorithm or a standard approved for particular country when data must be secured. Consult the Legal department and/or the appropriate government agency any time encryption



technology or encrypted information might cross government boundaries.

DES was developed by the National Bureau of Standards to provide a standard method for protecting sensitive commercial and unclassified data.

RSA is ANSI standard X9.44

The NSA is expected to provide additional guidelines for type 2 encryption techniques. Type 2 is a government-approved encryption standard for unclassified information.

Private Key Encryption—This method has the same binary number to encrypt and decrypt a message; therefore the single key must be secret for the message to remain secure.

Public Key Encryption—This method uses two keys system (Public and Private) which are related where the public key encrypts and the private key decrypts the message. The public-key infrastructure (PKI) allows the method to be used widely.

Rationale: The standard for SFA will be DES encryption and RSA Public Key.

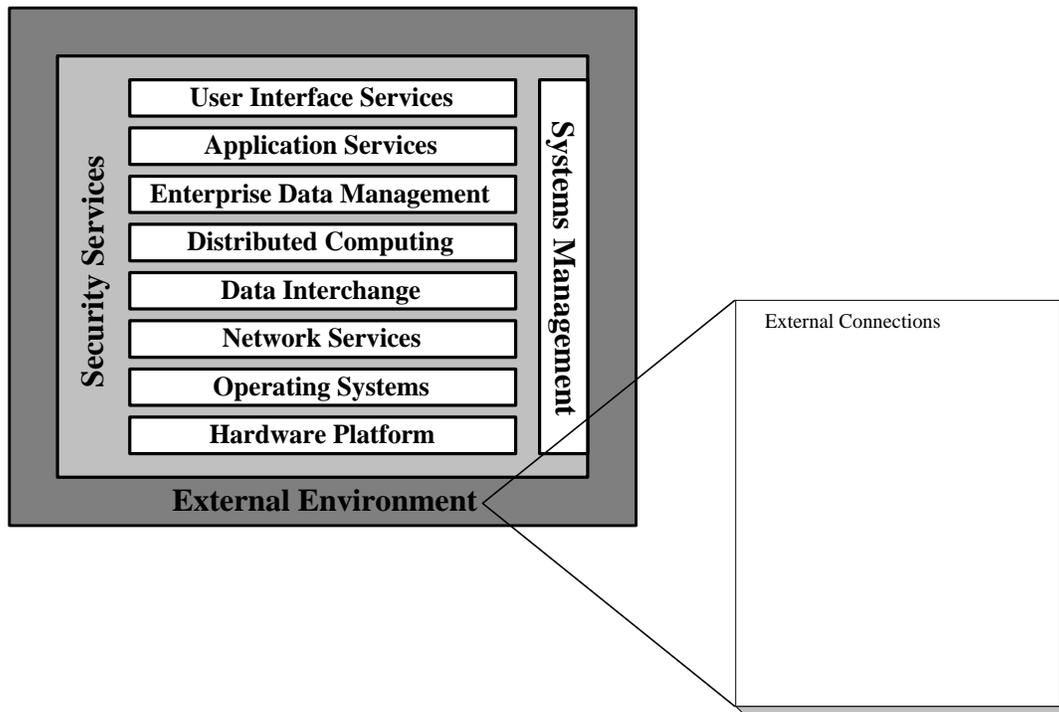
Virus Protection (Desktop) – McAfee, Norton Antivirus

Description: Platforms will have current anti-virus software installed and active to scan memory, boot sectors, attachments, and files. Multi-layered anti-virus protection may require a combination of several products to provide adequate protection across multi-platforms.

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving SFA Security Architecture.



4.10 External Environment



Brief Description

This section addresses external environment technologies and standards outside the scope of the TRM. The external environment includes technologies and standards beyond the physical and standards discussed previously. It encompasses WAN and transmission systems not normally encountered by SFA personnel.

- *External Connections*, such as wide area networks (Wanes), are divided into two parts. The first is trunk technology and switching. The customer generally purchases these services rather than investing in wide-area equipment and cable. The second is what the telephone industry refers to as the “local loop,” meaning the reach from the central office to the business or residence. Often the customer owns these assets.



Target Standards

Target Standards: External Environment

	FY 2002	FY 2003	FY 2004
External Connections	TBD	TBD	TBD

Approved Standards

External Connections – TBD

Description: See Exhibit 4-3: SFA Network Overview

Rationale: Standards will be continually identified to meet SFA's strategy to consolidate its WAN and further refine its Infrastructure Architecture while continuing the use of dedicated circuits and frame relay.



5 APPENDICES

Appendix A: Acronyms

Appendix B: Quick Reference Guide

Appendix C: Sources Referenced



APPENDIX A: ACRONYMS

ANSI	American National Standards Institute
API	application programming interface
CGI	Common Gateway Interface
CGM	Computer Graphics Metafile
COE	Common Operating Environment
COTS	commercial-off-the-shelf
CTI	computer telephony integration
DBMS	database management system
DES	Data Encryption Standard
DHCP	dynamic host configuration protocol
EIA	Electronics Industry Association
ETL	extract, transform, and load
FTP	File Transfer Protocol
GOTS	government-off-the-shelf
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization (also known as the International Standards Organization)
ITU-T	International Telecommunications Union–Telecommunications Standardization Sector
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol
JMS	Java Messaging Service
JPEG	Joint Photographic Expert Group
JSP	Java Server Pages
LAN	local area network
LDAP	lightweight directory access protocol
MAU	media access unit
MPEG	Motion Picture Experts Group
MSB	Minimum Baseline Standard



NIST National Institute of Standards Technology
ODBC open database connectivity
OMB Office of Management and Budget
OMG The Object Management Group
OLAP online analytical processing
OLTP online transaction processing
PCMCIA Personal Computer Memory Card International Association
PDA Personal Digital Assistant
PSTN Public Switched Telephone Network
RACF Resource Access Control Facility
RAID redundant array of independent disks
RDBMS relational database management system
RPC remote procedure call
RSA Rivest, Shamir, Adleman
SAN storage area network
SFA Student Financial Assistance
SLIP Serial Line Interface Protocol
SMTP Simple Message Transfer Protocol
SNMP Simple Network Management Protocol
TIA Telecommunications Industry Association
TOG The Open Group
TOGAF The Open Group Architectural Framework
TRM technical reference model
VPN Virtual Private Network
VRML Virtual Reality Modeling Language
WAN wide area network
XML Extensible Markup Language



APPENDIX A: APPENDIX B: QUICK REFERENCE GUIDE

This section provides quick reference to the SFA standards. More detailed descriptions of the policies and rationale of the standards are provided in the appropriate section of this document.

Target Standards: User Interface

	FY 2002	FY 2003	FY 2004
Web Browsers			
	HTML v4.0	HTML v4.0	HTML v4.0
	HTTP v1.0	HTTP v1.0	HTTP v1.0
Portals			
	Viador E-Portal Suite v6.1.1	WebSphere Custom Components	WebSphere Custom Components
Computer Telephony Integration			
	TBD	TBD	TBD
Audio Graphic Conferencing			
	TBD	TBD	TBD
Text-Based Conferencing			
	TBD	TBD	TBD
Video Conferencing			
	TBD	TBD	TBD

Target Standards: Application Services

	FY 2002	FY 2003	FY 2004
Desktop Tools			
	MS Office2000 Professional	MS Office2000 Professional	MS Office Professional
	MS Internet Explorer 5.5	MS Internet Explorer 5.5	MS Internet Explorer 5.5
Component Broker			
	IBM WebSphere/IIOP	IBM WebSphere/IIOP	IBM WebSphere/IIOP
Knowledge Management			
	Autonomy Knowledge Suite v3.1	Autonomy Knowledge Suite v3.1	Autonomy Knowledge Suite v3.1
Workflow Management			
	MQ Series Workflow v3.2.2	MQ Series Workflow v3.2.2	MQ Series Workflow v3.2.2



Content Management:

Interwoven Teamsite v4.2.1 Interwoven Teamsite v4.2.1 Interwoven Teamsite v4.2.1

Search Engine:

Autonomy Knowledge Suite v3.1 Autonomy Knowledge Suite v3.1 Autonomy Knowledge Suite v3.1

Target Standards: Enterprise Data Management

	FY 2002	FY 2003	FY 2004
Metadata Management			
	ISO 11179	ISO 11179	ISO 11179
Data Modeling			
	Sybase Power Designer 7.0	Sybase Power Designer 7.0	Sybase Power Designer 7.0
	Sterling Software CoolGen	Sterling Software CoolGen	
	Rational Suite 1.5 (Rose)	Rational Suite 1.5 (Rose)	Rational Suite 1.5 (Rose)
Database Management (Mod System & Data Mart)			
	Oracle 8i/8.05	Oracle 9i	Oracle 9i
	DB2	DB2	
Data Acquisition (Data Mart)			
	Informatica Power Center Server 1.7	Informatica Power Center Server 1.7	Informatica Power Center Server 1.7
Data Warehouse			
	MicroStrategy 7.0	MicroStrategy 7.0	MicroStrategy 7.0
End User Access (Data Mart)			
	Intelligence Server 7.0	Intelligence Server 7.0	Intelligence Server 7.0
	Web 7.0	Web 7.0	Web 7.0
	Broadcaster 6.5	Broadcaster 6.5	Broadcaster 6.5
	InfoCenter 6.5	InfoCenter 6.5	InfoCenter 6.5
	Agent 6.5	Agent 6.5	Agent 6.5
Imaging			
	TBD	TBD	TBD

Target Standards: Distributed Computing

FY 2002

FY 2003

FY 2004



Application Server			
	IBM WebSphere Enterprise Edition v3.5.5	IBM WebSphere Enterprise Edition v3.5.5	IBM WebSphere Enterprise Edition v3.5.5
	Oracle Application Server	Oracle Application Server	Oracle Application Server
Web Server			
	IBM IHS Server v1.3.12 (bundled with WebSphere application server)	IBM IHS Server v1.3.12 (bundled with WebSphere application server)	IBM IHS Server v1.3.12 (bundled with WebSphere application server)
	MS IIS	MS IIS	MS IIS
	Netscape Server	Netscape Server	Netscape Server
Middleware			
	MQ Series Server v5.2	MQ Series Server v5.2	MQ Series Server v5.2
	MQ Series Client v5.2	MQ Series Client v5.2	MQ Series Client v5.2
Application Specific			
	TBD	TBD	TBD

Target Standards: Data Interchange

	FY 2002	FY 2003	FY 2004
XML Server			
	Innovision XML Server	Innovision XML Server	Innovision XML Server
File Transfer			
	FTP, HTTP, SMTP (MIME), FTAM, and SNA	FTP, HTTP, SMTP (MIME), FTAM, and SNA	FTP, HTTP, SMTP (MIME), FTAM, and SNA
Electronic Data Interchange			
	XML (May 5 W3C XML Schema Recommendation)	XML (May 5 W3C XML Schema Recommendation)	XML (May 5 W3C XML Schema Recommendation)

Target Standards: Network Services

	FY 2002	FY 2003	FY 2004
Directory Servers			
	Netscape Directory Server	Netscape Directory Server	Netscape Directory Server
Internet and Transfer Protocols			
	TCP/IP	TCP/IP	TCP/IP
	SNA	SNA	
		VOIP	VOIP
Network Address Management			
	Static IP	Static IP	Static IP
	DHCP	DHCP	DHCP



Network Naming and Directory Services			
	DNS	DNS	DNS
Remote Access Services			
	Cisco Secure RADIUS	Cisco Secure RADIUS	Cisco Secure RADIUS
	Citrix	Citrix	Citrix
Virtual Private Network			
	CheckPoint VPN-1	CheckPoint VPN-1	CheckPoint VPN-1

Target Standards: Operating Systems

	FY 2002	FY 2003	FY 2004
Mainframe (Tier 1) Hosts/Servers			
	OS/390	OS/390	OS/390
	CICS	CICS	CICS
Mid Tier (Tier 2) Servers			
	HP/UX v11.0	HP/UX v11.0	HP/UX v11.0
	Windows NT	Windows NT	Windows NT
	Windows 2000	Windows 2000	Windows 2000
	Sun Solaris v2.6	Sun Solaris v2.6	Sun Solaris v2.6
Personal Computers (Tier 3)			
	Microsoft Windows 2000 Microsoft Windows 98	Microsoft Windows 2000	Microsoft Windows
Mobile Computers (Tier 3)			
	Microsoft Windows 2000	Microsoft Windows 2000	Microsoft Windows

Target Standards: System Management

	FY 2002	FY 2003	FY 2004
User Support Services			
	TBD	TBD	TBD
Configuration Management			
	Computer Associates Harvester Change Manager (Mid-Tier)	Computer Associates Harvester Change Manager (Mid-Tier)	Computer Associates Harvester Change Manager (Mid-Tier)
	Computer Associates Endeavor (Mainframe)	Computer Associates Endeavor (Mainframe)	Computer Associates Endeavor (Mainframe)
	Rational ClearCase v4.1 (Non-mainframe)	Rational ClearCase v4.1 (Non-mainframe)	Rational ClearCase v4.1 (Non-mainframe)
	Rational ClearQuest 2001 v4.0 (Mid-Tier)	Rational ClearQuest 2001 v4.0 (Mid-Tier)	Rational ClearQuest 2001 v4.0 (Mid-Tier)



Inventory Management			
	Self-built solution	Self-built solution	Self-built solution
Operations Management			
	Computer Associates CA-7 (Mainframe)	Computer Associates CA-7 (Mainframe)	Computer Associates CA-7 (Mainframe)
	BMC Control D (Printing)	BMC Control D (Printing)	BMC Control D (Printing)
	BMC Control M/R (Mainframe)	BMC Control M/R (Mainframe)	BMC Control M/R (Mainframe)
	Hewlett Packard OpenView (Network Monitor)	Hewlett Packard OpenView (Network Monitor)	Hewlett Packard OpenView (Mid-tier)
Load Balancing			
	IBM WebSphere Performance Pack v3.0	IBM WebSphere Performance Pack v3.0	IBM WebSphere Performance Pack v3.0
	Cisco Director	Cisco Director	Cisco Director
Network Inventory and Distribution Services			
	Microsoft Software Management System (SMS)	Microsoft Software Management System (SMS)	Microsoft Software Management System (SMS)
	Lotus Notes	Lotus Notes	Lotus Notes
	Candle Management	Candle Management	Candle Management

Target Standards: Security Services

	FY 2002	FY 2003	FY 2004
Digital Certificate Server Services			
	Netscape Certificate Server	Netscape Certificate Server	Netscape Certificate Server
Firewall Services			
	CheckPoint Firewall-1	CheckPoint Firewall-1	CheckPoint Firewall-1
Access Control			
	RACF (Mainframe)	RACF (Mainframe)	RACF (Mainframe)
	BMC Control SA	BMC Control SA	BMC Control SA
Audit Trail Creation			
	System Log File	System Log File	System Log File
Authentication			
	RACF (Mainframe)	RACF (Mainframe)	RACF (Mainframe)
	BMC Control SA (Mainframe)	BMC Control SA (Mainframe)	BMC Control SA (Mainframe)
	TBD (Mid-tier)	TBD (Mid-tier)	TBD (Mid-tier)
Database Security Services			
	RACF (Mainframe)	RACF (Mainframe)	RACF (Mainframe)



	TBD (Mid-tier)	TBD (Mid-tier)	TBD (Mid-tier)
Electronic Signatures/Non-repudiation			
	TBD		
Host Intrusion Detection			
	TBD	TBD	TBD
	TBD	TBD	TBD
	TBD	TBD	TBD
Network Intrusion Detection			
	RealSecure	RealSecure	RealSecure
Physical Security			
	TBD		
Encryption			
	Secure Socket Layer	Secure Socket Layer	Secure Socket Layer
	BSAFE	BSAFE	BSAFE
Virus Protection (Desktop)			
	McAfee	McAfee	McAfee
	Norton Antivirus	Norton Antivirus	Norton Antivirus

Target Standards: External Environment

	FY 2002	FY 2003	FY 2004
External Connections			
	TBD	TBD	TBD



APPENDIX C: SOURCES REFERENCED

Documents:

- Enterprise Information Technology Architecture Framework: Business Drivers and Architecture Principles October 8, 1998
- Office of Management and Budget (OMB) Circular A-130 Appendix III
- Office of Student Financial Assistance Guide to Information Security and Privacy
- Security Architecture
- SFA Information Security General Minimum Security Baseline Standards
- SFA Information Technology Architecture Framework – Phase I
- SFA Software Engineering Handbook