

Department of Education
SFA IT Management



SFA Technology Policy Guide ³/₄ v1.5



TABLE OF CONTENTS

1	Introduction	1
1.1	Legislative Compliance	1
1.2	Standards.....	1
1.3	Authority and Governance.....	2
2	Conceptual Architecture.....	2
3	Technical Reference Model.....	3
4	Technology Policies and Standards.....	5
4.1	User Interface Services	6
4.1.1	Web Browsers.....	7
4.1.2	Portals.....	7
4.1.3	Computer Telephony Integration.....	8
4.1.4	Audiographic Conferencing.....	8
4.1.5	Text-Based Conferencing.....	8
4.1.6	Video Conferencing.....	9
4.2	Application Services	10
4.2.1	Desktop Tools.....	10
4.2.2	Component Brokers.....	12
4.2.3	Knowledge Management.....	12
4.2.4	Workflow Management.....	13
4.2.5	Content Management.....	14
4.2.6	Search Engines.....	15
4.3	Enterprise Data Management.....	15
4.3.1	Metadata Management	16
4.3.2	Data Modeling.....	17
4.3.3	Database Management.....	18
4.3.4	Data Acquisition	18
4.4	Distributed Computing.....	21
4.4.1	Application Server Services.....	21



SFA Technology Policy Guide ¾ Phase I

4.4.2	Web Server Services	22
4.4.3	Middleware.....	23
4.5	Data Interchange	24
4.5.1	XML Server Services.....	25
4.5.2	File Transfer	25
4.5.3	Electronic Data Interchange	26
4.6	Network Services	27
4.6.1	Directory Server Services.....	28
4.6.2	Internet and Transport Protocols.....	29
4.6.3	Network Address Management Services.....	29
4.6.4	Network Naming and Directory Services	30
4.6.5	Remote Access Services	31
4.6.6	Virtual Private Network	32
4.7	Operating Systems	33
4.7.1	Mainframe (Tier 1) Hosts/Servers	34
4.7.2	Mid-Tier (Tier 2) Servers.....	35
4.7.3	Personal Computers (Tier 3)	36
4.7.4	Mobile Workstations (Tier 3).....	36
4.8	Systems Management.....	37
4.8.1	User Support Services	38
4.8.2	Configuration Management.....	38
4.8.3	Inventory Management.....	39
4.8.4	Operations Management	39
4.8.5	Load Balancing.....	40
4.8.6	Network Inventory and Distribution.....	41
4.9	Security Services.....	42
4.9.1	Digital Certificate Server Services	42
4.9.2	Firewalls.....	43
4.9.3	Access Control.....	44
4.9.4	Audit Trail Creation and Analysis	45



SFA Technology Policy Guide ¾ Phase I

4.9.5	Authentication.....	46
4.9.6	Database Security.....	47
4.9.7	Electronic Signature/Non-Repudiation	48
4.9.8	Host Intrusion Detection.....	48
4.9.9	Network Intrusion Detection	49
4.9.10	Physical Security.....	49
4.9.11	Privacy and Integrity (Encryption)	50
4.9.12	Virus Prevention.....	51
4.10	External Environment.....	52
4.10.1	External Connections	52
5	Acronyms.....	54



1 INTRODUCTION

This document will outline the technology policies and standards of the U.S. Department of Education Student Financial Assistance (SFA) modernization.

The SFA architecture follows The Open Group Architectural Framework (TOGAF), which defines the process of developing an architecture and describes the fundamental technologies comprising the target architecture.

1.1 Legislative Compliance

An information technology architecture in compliance with Clinger-Cohen legislation and Office of Management and Budget (OMB) guidance 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 with the pertinent aspects of Clinger-Cohen legislation and OMB Circular No. A-130.

1.2 Standards

Producers and consumers of information technology are increasingly recognizing that standards, whether open systems standards or proprietary standards, enable the use and proliferation of technology. Open systems products and technologies have been designed and implemented according to open interfaces. Interfaces are considered open if their specifications are readily available to all suppliers, service providers, and users and are revised only with timely notice and by a public process. Several organizations have developed and continue to maintain standards for open systems and are cited in this document:

American National Standards Institute (ANSI)

Electronics Industry Association (EIA)

Institute of Electrical and Electronics Engineers (IEEE)

Internet Engineering Task Force (IETF)

International Organization for Standardization; also known as the International Standards Organization (ISO)

International Telecommunications Union–Telecommunications Standardization Sector (ITU-T)

National Institute of Standards and Technology (NIST)

The Object Management Group (OMG)

Telecommunications Industry Association (TIA)

The Open Group (TOG)



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 pertinent 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 and harmonize with the SFA IT 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:

1. **The architecture must support the business:** The enterprise architecture and standards will be designed to (1) support and optimize SFA operations, (2) be highly flexible to accommodate future business changes, and (3) help ensure the overall success of the SFA business.
2. **Reengineer business processes and supporting IT together:** New information systems will be implemented after work processes have been analyzed, simplified, or otherwise redesigned as appropriate, in compliance with Clinger-Cohen legislation and Raines’ rules.
3. **Enhance and simplify access to information:** Timely access to information and 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.
4. **Design integration and reuse into IT initiatives:** SFA IT initiatives will be designed to maximize reuse of existing code and databases.
5. **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.
6. **No vendor bias:** 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 its architecture standards.
7. **Solutions preference:** Where 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.
8. **Reduce integration complexity:** Products, tools, designs, applications, and methods will be selected to reduce integration and infrastructure complexity.

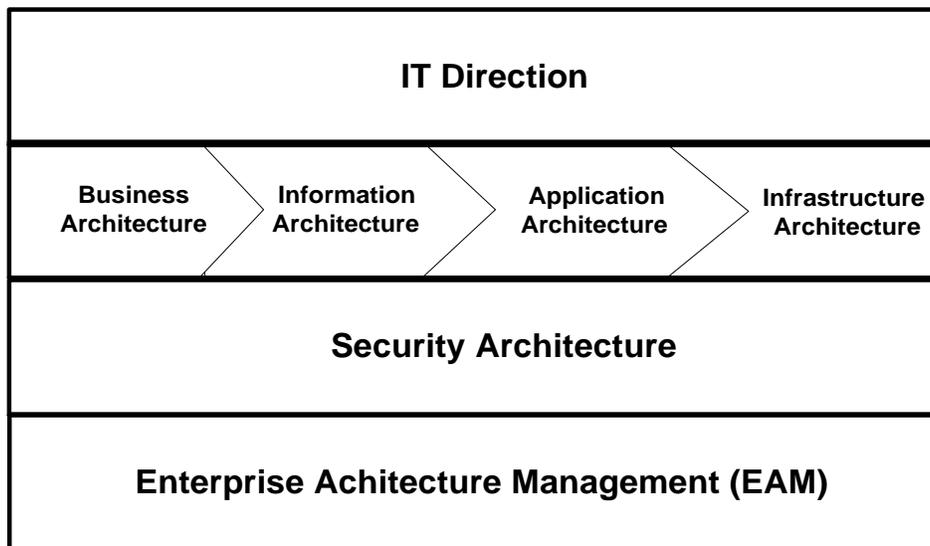


SFA Technology Policy Guide ¾ Phase I

9. **Architecture enforcement:** The information systems and technology infrastructure implemented by SFA will be compliant with the SFA Enterprise Architecture and Common Operating Environment (COE).
10. **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. The diagram below shows the infrastructure architecture and management functions and how they provide the foundation for the IT direction.

Exhibit 2-1: SFA's IT Components



3 TECHNICAL REFERENCE MODEL

The basis for the guide is the Technical Reference Model (TRM), which is a conceptual representation of services and interfaces in the information system. Its purpose is to provide a context for understanding how the disparate technologies required to implement information management relate to each other.

This Technology Policy Guide is written using this model as a guide. The SFA TRM is depicted in Exhibit 3-1. The major service areas in the SFA TRM are:

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



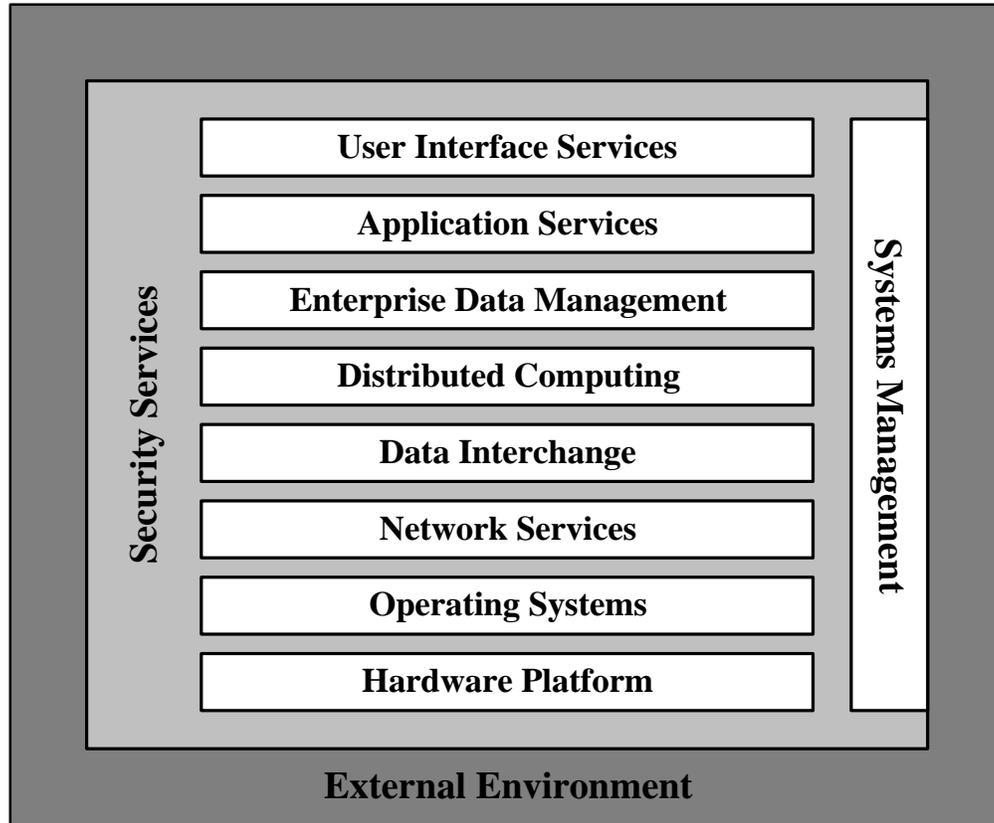
SFA Technology Policy Guide ¾ Phase I

- **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 backbone (network).
- **Operating Systems**—technologies that enable computers to manage resources and memory and run programs.
- **Hardware Platform**—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.
- **Systems Management**—technologies and practices that enable the monitoring and control of the SFA information technology infrastructure.
- **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. Security services are integrated into each major service area. Systems management is influenced by every other service area.



Exhibit 3-1: Technical Reference Model



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 technology policy, the standards, and a target timeframe for implementing the standards.

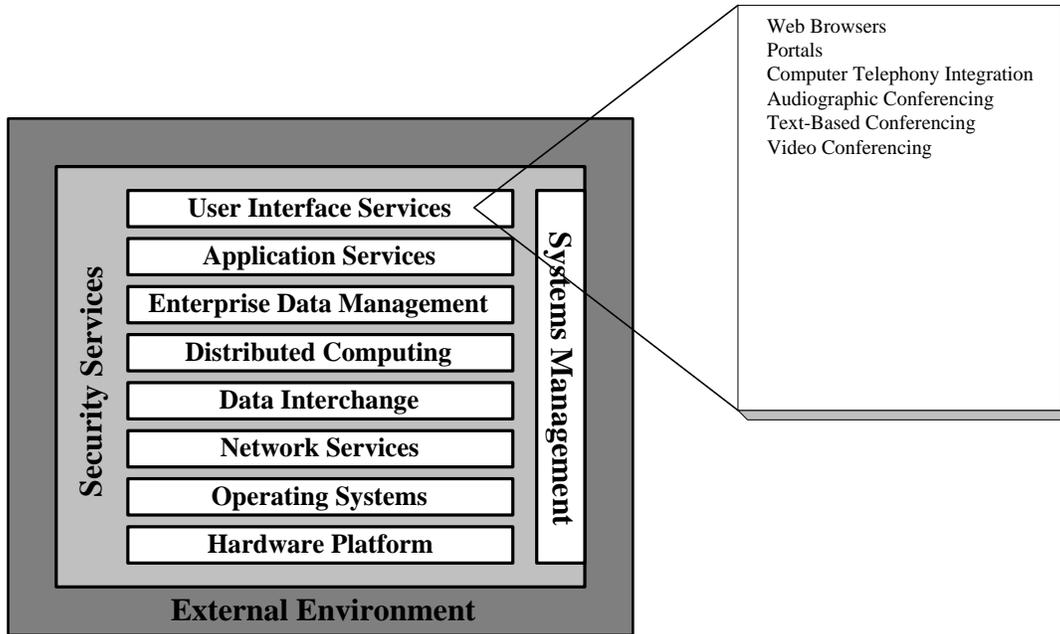
Each technology policy and standard will have a timeline table as shown below defining the standard product or products that are to be used by SFA now and in the future. The timeline will be updated periodically to reflect changes in SFA business objectives and emerging technologies.

4.1.1.1 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003



4.1 User Interface Services



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

- Graphical client-server services, which define the relationships between client and server processes operating graphical user interface displays, usually within a network.
- Display objects services, which define characteristics of display elements such as color, shape, size, movement, graphics context, user preferences, font management and interactions among display elements.
- Window management services, which define how windows are created, moved, stored, retrieved, removed, and related to each other.
- Dialogue support services, which translate the data entered for display to that which is actually displayed on the screen (e.g., cursor movements, keyboard data entry, external data entry devices).
- Character-based services, which deal with support for non-graphical terminals.

Window system services include the visual display of information on a screen, support for pointing to an object on the screen using a pointing device such as a mouse or touch-screen, and the manipulation of a set of objects on the screen through the pointing device or through keyboard entry.



SFA Technology Policy Guide ¾ Phase I

4.1.1 Web Browsers

Web browsers are client applications that provide a GUI to the Internet through HyperText Markup Language (HTML), allowing users to view and interact with applications and documents made up of various data types, such as text, graphics, and audio. These services also provide support for navigation within and across documents through the use of links embedded into the document content. Technologies such as Java allow users to interact with existing legacy applications through these browsers.

4.1.1.1 Technology Policy

SFA web browser services will provide server communication, communication security, presentation services, scripting, and run-time services. SFA products should support HTML and Java technologies. SFA customers will use a variety of browsers that SFA will have no control over, including text-based browsers for use with older computers (e.g., those using Windows 3.11) such as Lynx. Support does not imply full functionality of features that are available only with more recent standards of products.

4.1.1.2 Standards

For external users accessing SFA information via a Web browser, SFA language and protocol standards are HTML v4.0 and HTTP v1.0.

4.1.1.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	HTML v4.0	HTML v4.0	HTML v4.0
	HTTP v1.0	HTTP v1.0	HTTP v1.0

4.1.2 Portals

The portal component of the SFA Internet architecture will provide a Web-based user-customizable interface as a point of access to a wide variety of data sources, including content, documents, and applications. The portal will provide integrated access, authorization, and authentication to SFA services through the Web, providing the users with a personalized view.

4.1.2.1 Technology Policy

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.

4.1.2.2 Standards

No published industry standard identified.

4.1.2.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	Viador E-Portal Suite	Viador E-Portal Suite	Viador E-Portal Suite



SFA Technology Policy Guide ¾ Phase I

4.1.3 Computer Telephony Integration

Computer telephony integration (CTI) integrates computers, networks, PBX switches, and other equipment such as PC-based answering machines, faxes, and pagers. CTI enables automated handling of telephone calls, automatic call back, initiation of workflow, guaranteed quality of service for customers, and sophisticated task tracking.

4.1.3.1 Technology Policy

SFA is currently developing its customer relationship management (CRM) strategy, which will include CTI.

4.1.3.2 Standards

Industry standards vary per platform; more detail will be provided as the standards are selected.

4.1.3.3 Target Standards and Timeframe*

As Is	2000/2001	2001/2002	2002/2003
	TBD		

* Note: SFA currently has a variety of solutions spread across multiple call centers. This time horizon will evolve over future releases of this document.

4.1.4 Audio graphic Conferencing

Audio graphic conferencing provides a more cost-effective method of conferencing when seeing the conference participants is not required. The audio portion is typically a telephone conference call. The graphics portion is provided over the network and displays an image that can be modified by all participants. The graphics portion provides the enhanced capability beyond a telephone conference call. The graphic is usually referred to as a whiteboard.

4.1.4.1 Technology Policy

TBD

4.1.4.2 Standards

Multiple industry standards exist; no recommendation has been made.

4.1.4.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TBD		

4.1.5 Text-Based Conferencing

Text-based conferencing requires the lowest network bandwidth of the three types of conferencing discussed. It provides a mechanism that allows conference participants to view



SFA Technology Policy Guide ¾ Phase I

each participant’s input. One of the features of the textual conference is that the text can be saved and referred to at a later time.

4.1.5.1 Technology Policy

The selection of a product is pending.

4.1.5.2 Standards

To be identified.

4.1.5.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TBD		

4.1.6 Video Conferencing

Video conferencing enables people at different sites to simulate face-to-face meetings in real time. Current video conferencing equipment 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 incorporate equipment that enables sharing of graphics and electronic documents. Personal computer video conferencing links individuals rather than groups. Personal computer application sharing is sometimes combined with personal computer video conferencing. There are two standards—high-end high-quality video conferencing and low-end PC-based dedicated studio environments—but no sanctioned personal computer application for general use.

4.1.6.1 Technology Policy

TBD

4.1.6.2 Standards

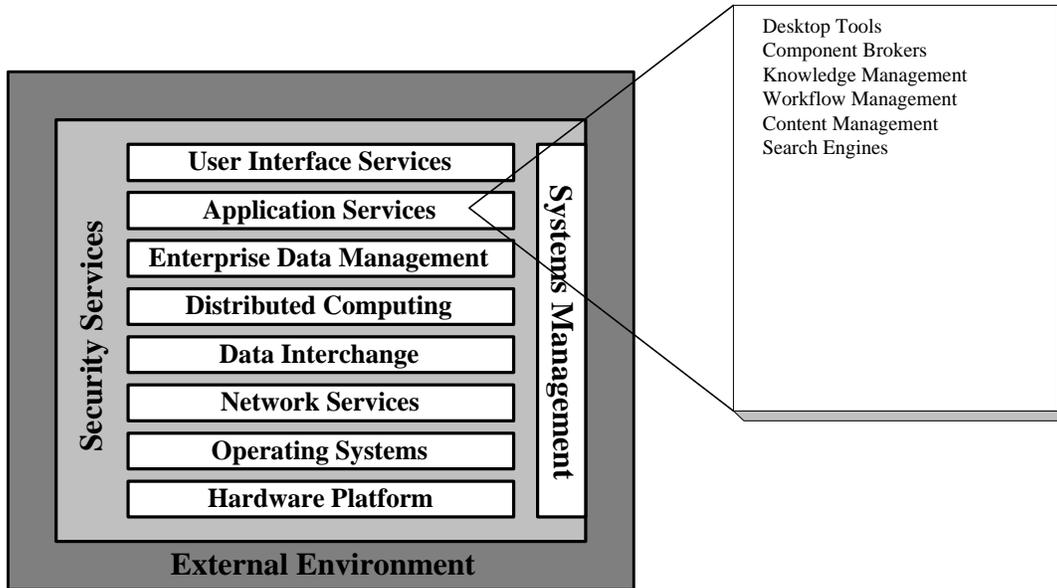
No published industry standard identified.

4.1.6.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
PictureTel	TBD		



4.2 Application Services



Application services are technologies that provide support for the business processes of an organization, including transaction services and software development environment. These services provide the means by which an organization can deploy network-centric applications in the Internet and intranet environments, encompassing 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 Office2000 suite of products in the current SFA Seat Management project.

4.2.1 Desktop Tools

Standard office productivity tools consist of those applications and software components supporting a standard office automation environment. They include user interface, word processing, spreadsheets, presentation graphics, and web browsers.

In choosing standard enterprise applications, software products that are designed to international or national standards are preferred over those designed to a lower standard. Additionally, COTS software will always be preferred over government-off-the-shelf (GOTS) software produced by other Federal agencies or private companies working under contract for the government. As time passes, business processes change and technology advances, which can render sanctioned productivity tools inadequate or obsolete.



SFA Technology Policy Guide ¾ Phase I

4.2.1.1 Technology Policy

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.

4.2.1.2 Standards

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 Exhibit 4-1.

Exhibit 4-1: Common File Formats

Document Type	Standard/Vendor Format	Recommended File Name Extension	Formats Supported	Reference
Plain Text	ASCII Text	.txt		
Compound Document	Acrobat	.pdf		Vendor
Document	HTML	.htm		IETF
	MS Word	.doc		Vendor
	Rich Text Format	.rtf		Vendor
Presentation	MS PowerPoint	.ppt		Vendor
	MS Excel	.xls		Vendor
Graphics	CGM			FIPS Publ. 128-1, 1993
	JFIF			JPEG
Audio	Wave (WAV)	.wav		
	Audio-Video Interleaved	.avi		
	Audio UNIX (AU)			
Video	MPEG, MPEG2			MPEG
Internet	HTML	.htm		IETF
Compressed	WINZip	.zip		
Database	Dbase	.dbf and .mdb		Vendor

4.2.1.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	MS Office2000 Professional	MS Office2000 Professional	MS Office Professional
	MS Internet Explorer 4.01	MS Internet Explorer 4.5	MS Internet Explorer



SFA Technology Policy Guide ¾ Phase I

4.2.2 Component Brokers

The component broker provides object-based functionality to the application server component. An object-based capability provides a standard model for object state and behavior accessible through object methods. Component broker is an enterprise solution for distributed computing, providing a scalable, manageable environment for developing and deploying distributed component-based solutions.

Primarily, the component broker is an object server. It comes with 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. The run-time package provides a server in which business object components run and are managed through a set of management tools.

4.2.2.1 Technology Policy

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.

4.2.2.2 Standards

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).

4.2.2.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	IBM WebSphere/ IIOP	IBM WebSphere/ IIOP	IBM WebSphere/ IIOP

4.2.3 Knowledge Management

The knowledge management component provides information search and retrieval capability. This component offers 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.

4.2.3.1 Technology Policy

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 be able to support a thesaurus query if a thesaurus is loaded into the environment.



SFA Technology Policy Guide ¾ Phase I

4.2.3.2 Standards

No published industry standard identified.

4.2.3.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	Autonomy Knowledge Suite	Autonomy Knowledge Suite	Autonomy Knowledge Suite

4.2.4 Workflow Management

Workflow management technology 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 work lists of people involved.

As applications continue to increase in sophistication, workflow services are being added to desktop applications. Often, mail systems, groupware tools, and electronic forms packages can provide some workflow functionality.

4.2.4.1 Technology Policy

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

4.2.4.2 Standards

No standards specific to workflow products 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.



SFA Technology Policy Guide ¾ Phase I

4.2.4.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	MQSeries Workflow, Version 3.2.2	MQSeries Workflow, Version 3.2.2	MQSeries Workflow, Version 3.2.2

4.2.5 Content Management

The content management component 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 artifact. The individual content versions are associated with Web site configurations or releases.
- Categorization and Publishing—manages groups of content artifacts according to user-defined criteria and supports publishing of these content artifacts.
- 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 artifacts that were delivered from the development environment to the production environment.

4.2.5.1 Technology Policy

Content management will accelerate the way SFA will move 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 taking the frustration and unpredictability out of the process. Content management will includes replication and syndication featuring with rules-based distribution of all content across the SFA network. Content management 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. Use of advanced security options will provide a powerful syndication solution for the SFA enterprise Web environment.

4.2.5.2 Standards

No published industry standard identified.



SFA Technology Policy Guide ¾ Phase I

4.2.5.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	Interwoven Teamsite, Version 4.2.1	Interwoven Teamsite, Version 4.2.1	Interwoven Teamsite

4.2.6 Search Engines

Search engines will provide search and retrieval capability on different data groups in an Internet-based environment.

4.2.6.1 Technology Policy

The search engine provides pattern-matching technology that will enable SFA to efficiently identify and encode unique key words within text documents. Then the search engine seeks out and uncovers the presence of similar concepts in volumes of content, such as a set of Web sites, news feed, or an e-mail archive.

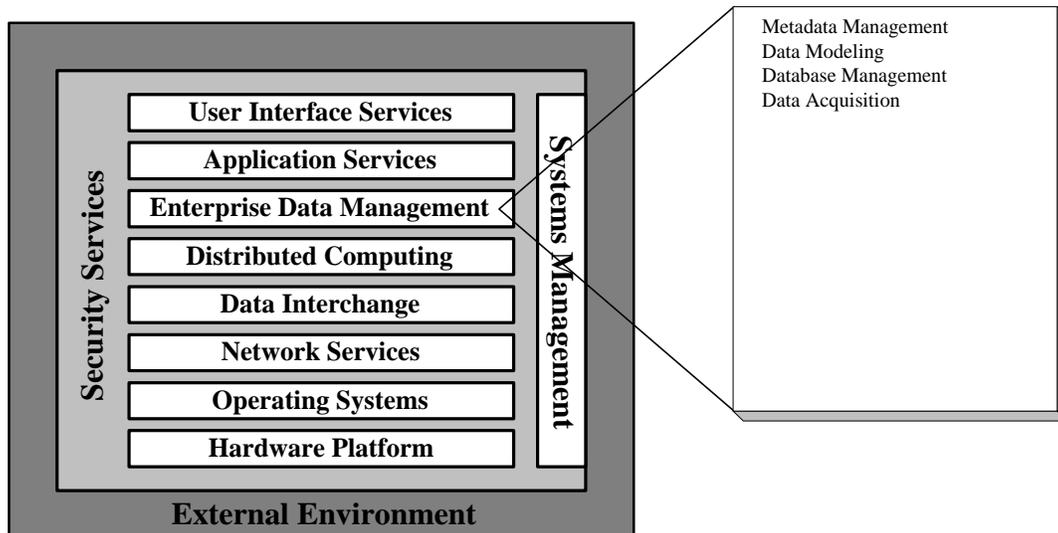
4.2.6.2 Standards

No published industry standard identified.

4.2.6.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	Autonomy	Autonomy	Autonomy

4.3 Enterprise Data Management



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



SFA Technology Policy Guide ¾ Phase I

- Enterprise data dictionary/repository services, which allow data administrators and information engineers to access and modify data about data (i.e., metadata). Metadata may 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).
- DBMS services, which provide 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. 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 warehouse services, which, after extract, transform, and load (ETL), provide read-only, time-dependent data for end user access, online analysis, and reporting.
- File management services, which provide data management through file access methods.

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”).

4.3.1 Metadata Management

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.



SFA Technology Policy Guide ¾ Phase I

- 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.

4.3.1.1 Technology Policy

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.

4.3.1.2 Standards

SFA metadata management will comply with the ISO 11179 standard.

4.3.1.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TBD		

4.3.2 Data Modeling

The purpose of a data model is to identify and clearly define the entities, in which the business must keep data, and to identify and clearly define the important associations between those entities. Different parts of a business are interested in the same entities, but there tend to be conflicting meanings, states, business rules, names, etc. Until these differences are resolved as a part of building the data model, there can be no meaningful progress toward building shared, subject-oriented databases that can greatly reduce information float, redundant and unnecessary work, redundant and unnecessary data and programming, and excessive time and cost in conducting the business. A conceptual data model lays the foundation not only for building shared databases but also for reengineering the business. Collapsing information and material float within and between business processes are the keys to improving the way a business works. The principle of shared data is one of the most fundamental, yet astonishingly under-utilized, in business today.

4.3.2.1 Technology Policy

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.

4.3.2.2 Standards

No published industry standard identified.



SFA Technology Policy Guide ¾ Phase I

4.3.2.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	Sybase Power Designer 7.0	Sybase Power Designer 7.0	Sybase Power Designer 7.0

4.3.3 Database Management

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.

4.3.3.1 Technology Policy

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

4.3.3.2 Standards

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.

4.3.3.3 Target Standards and Timeframe

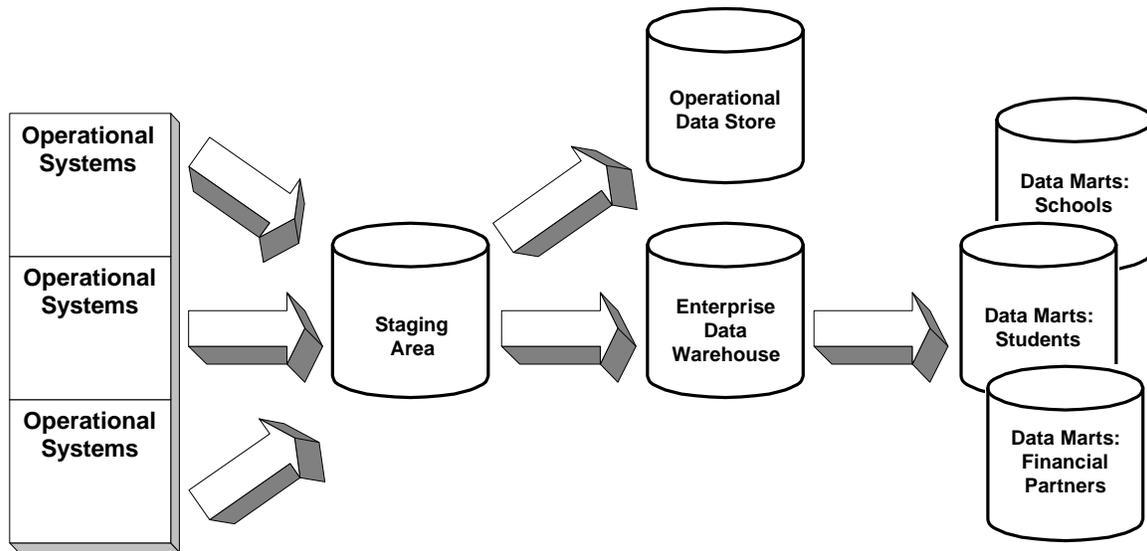
As Is	2000/2001	2001/2002	2002/2003
	Oracle 8i/8.05	Oracle 8i	Oracle 8i
	DB2	DB2	

4.3.4 Data Acquisition

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. The diagram below details the flow of data in the data warehouse architecture from the data sources to the data marts.



SFA Technology Policy Guide ¾ Phase I



4.3.4.1 Access to Source Data (ETL)

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.

4.3.4.2 Technology Policy

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.

4.3.4.3 Standards

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.

4.3.4.4 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	Informatica Power Center Server 1.7	Informatica Power Center Server 1.7	Informatica Power Center Server 1.7

4.3.4.5 Data Warehouse

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:



SFA Technology Policy Guide ¾ Phase I

- 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.

4.3.4.6 Technology Policy

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.

4.3.4.7 Standards

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

4.3.4.8 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TBD		

4.3.4.9 End User Access

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.

4.3.4.10 Technology Policy

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



SFA Technology Policy Guide ¾ Phase I

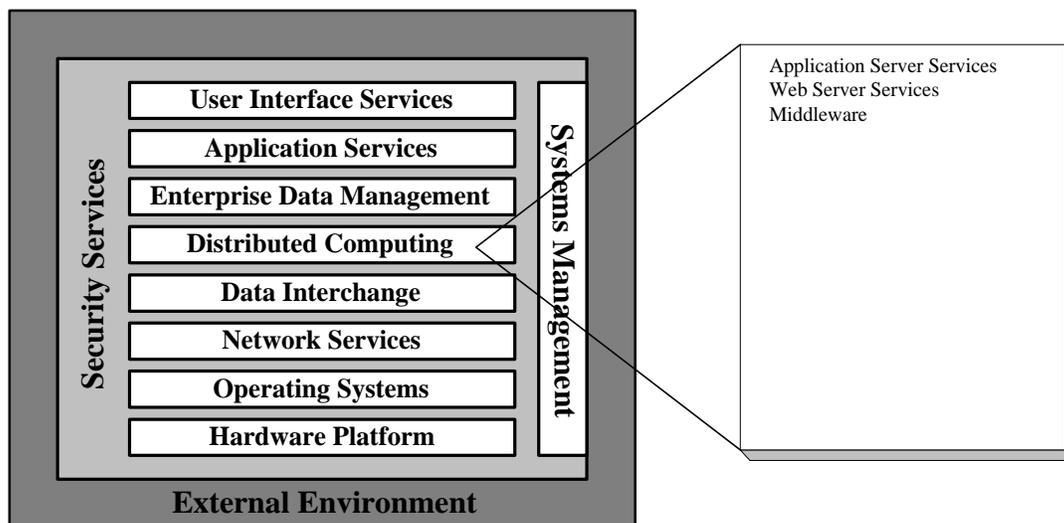
4.3.4.11 Standards

No published industry standard identified.

4.3.4.12 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	Intelligence Server 7.0 Web 7.0 Broadcaster 6.5 InfoCenter 6.5 Agent 6.5	Intelligence Server 7.0 Web 7.0 Broadcaster 6.5 InfoCenter 6.5 Agent 6.5	Intelligence Server 7.0 Web 7.0 Broadcaster 6.5 InfoCenter 6.5 Agent 6.5

4.4 Distributed Computing



Distributed computing services are required to operate similarly across physically and even geographically 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.

4.4.1 Application Server Services

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 the following services:



SFA Technology Policy Guide ¾ Phase I

thread management; database connection pooling; persistence; memory management; logging; naming and directory services; security, including access control (such as authentication) and secure connections; application management; transaction support; automatic load balancing; and automatic fail-over support.

4.4.1.1 Technology Policy

SFA application servers must 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.

4.4.1.2 Standards

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.

4.4.1.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	IBM WebSphere Enterprise Edition, Version 3.0.2	IBM WebSphere Enterprise Edition, Version 3.5	IBM WebSphere Enterprise Edition, Version 3.5

4.4.2 Web Server Services

Web server services enable organizations to manage and publish information and deploy network-centric applications over the Internet (public) and intranet (private) environments.

4.4.2.1 Technology Policy

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.



SFA Technology Policy Guide ¾ Phase I

4.4.2.2 Standards

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.

4.4.2.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	IBM IHS Server bundled with WebSphere application server	IBM IHS Server bundled with WebSphere application server	IBM IHS Server bundled with WebSphere application server

4.4.3 Middleware

Message-oriented middleware (MOM) provides a standard API across hardware and operation system platforms and networks. 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.

4.4.3.1 Technology Policy

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



SFA Technology Policy Guide ¾ Phase I

every message to the correct location with table-driven rules bases, and transform data on the fly across DB2 and Oracle application systems.

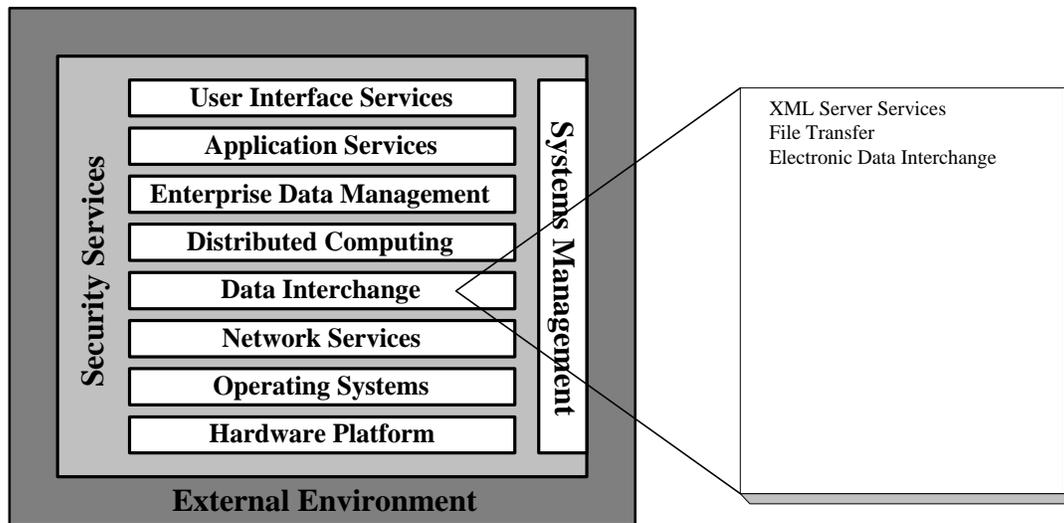
4.4.3.2 Standards

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.

4.4.3.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	MQSeries Server, Version 2.0	MQSeries Server, Version 2.0	MQSeries Server, Version 2.0
	MQSeries Client, Version 5.1	MQSeries Client, Version 5.1	MQSeries Client, Version 5.1

4.5 Data Interchange



Data interchange services provide specialized support for the interchange 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 (heterogeneous) platforms. Data interchange services include:

- Document generic data typing and conversion services, which are supported by specifications for encoding the data (e.g., text, pictures, numeric, special characters) and both the logical and visual structures of electronic documents, including compound documents.



SFA Technology Policy Guide ¾ Phase I

- Graphics data interchange services, which are supported by device-independent descriptions of picture elements for vector-based graphics and descriptions for raster-based graphics.
- Specialized data interchange services, which are supported by specifications that describe data used by specific vertical markets.
- Electronic data interchange services, which are used to create an electronic environment for conducting commerce and achieving significant gains in quality, responsiveness, and savings afforded by such an environment.

4.5.1 XML Server Services

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.

4.5.1.1 Technology Policy

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.

4.5.1.2 Standards

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.

4.5.1.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	Innovision XML Server	Innovision XML Server	Innovision XML Server

4.5.2 File Transfer

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



SFA Technology Policy Guide ¾ Phase I

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.

4.5.2.1 Technology Policy

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.

4.5.2.2 Standards

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

4.5.2.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
Hummingbird	Hummingbird	Hummingbird	Hummingbird

4.5.3 Electronic Data Interchange

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.

4.5.3.1 Technology Policy

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



SFA Technology Policy Guide ¾ Phase I

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.

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).

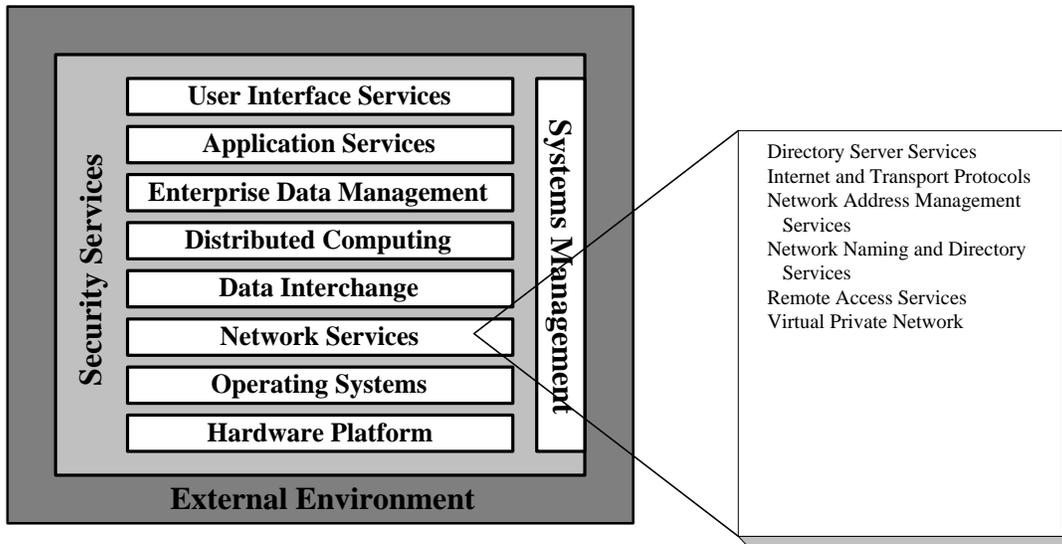
4.5.3.2 Standards

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

4.5.3.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
To be identified	XML	XML	XML

4.6 Network Services





SFA Technology Policy Guide ¾ Phase I

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:

- Data communications, which include interfaces and protocols for reliable, transparent, end-to-end data transmission across communications networks.
- Electronic-mail services, which include the capability to send, receive, forward, store, display, retrieve, prioritize, authenticate and manage messages.
- Distributed data services, which provide access to, and modification of, data/metadata in remote or local databases.
- Distributed name services, which provide a means for unique identification of resources within a distributed computing system.
- Distributed time services, which provide synchronized time coordination as required among distributed processes in different time zones.
- Remote process (access) services, which provide the means for dispersed applications to communicate across a computer network. These services facilitate program-to-program communications regardless of their distributed nature or operation on heterogeneous platforms.
- Remote print spooling and output distribution services, which provide the means for printing output remotely, including printer and media selection, use of forms, security, and print queue management.

4.6.1 Directory Server Services

Directory servers act as 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.

4.6.1.1 Technology Policy

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.

4.6.1.2 Standards

No published industry standard identified.

4.6.1.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TBD		



SFA Technology Policy Guide ¾ Phase I

4.6.2 Internet and Transport Protocols

Data network interoperability addresses the need to deliver 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.

4.6.2.1 Technology Policy

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.

4.6.2.2 Standards

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. TCP/IP has become so popular that the TCP/IP addressing scheme is becoming insufficient. Migration to IP version 6 (IPv6) will be gradual but will consume considerable effort for network management organizations. IPv6 has vastly improved security capabilities that IPv4 fails to deal with well or at all. IP addressing will need to be expanded, and this expansion will have a direct impact in network-wide naming standards. With IPv6, for example, the IP address is expanded from 32 bits to 128 bits. Dynamic host configuration protocol (DHCP; RFCs 1533, 1534, and 1541), a standard method of connection across Internet service providers, should aid in the migration.

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.

4.6.2.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TCP/IP	TCP/IP	TCP/IP
	SNA	SNA	
		VOIP	VOIP

4.6.3 Network Address Management Services

Addressing is the process of giving each network element and user an identity that is used by network components to determine the location of objects in the network. For most networks, some form of name and address is an integral component of their operation. For the most part, naming schema and addressing schema are unrelated. A name is used to identify an object; an address provides the means to locate the object in the network. When an object is relocated on the network, its network address changes; however, the object name may remain the same. The



SFA Technology Policy Guide ¾ Phase I

naming scheme assigns network-location-independent identifiers to objects; the addressing scheme assigns addresses to network locations.

Two critical issues involving IP address space management are address space depletion and the increasing cost of address administration. Network address translation (NAT) and DHCP are designed to address these issues. A NAT translates addresses on an as-needed basis from a finite registered Internet address space to a user-defined, but infinite, unregistered address space, thereby creating the appearance of more addresses than are really available. A primary limitation is over-subscription from users simultaneously requesting more registered addresses than are available. DHCP also “leases” addresses on an as-needed basis, but the period of the lease is typically much longer than that of a NAT. It is designed to eliminate the burden of managing constant address changes.

4.6.3.1 Technology Policy

SFA employs DHCP as its standard network address management service; 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.

4.6.3.2 Standards

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

4.6.3.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	DHCP	DHCP	DHCP

4.6.4 Network Naming and Directory Services

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. The Internet DNS is an open, standard naming service supported by the IETF. Although there are stand-alone systems such as DNS that implement a naming service, most are integrated within other services such as file systems and e-mail. In a directory service, objects are identified and retrieved based on their attributes, where one of the attributes is its name. This service provides the additional capability of searching for all objects that have one or more particular attributes.



SFA Technology Policy Guide ¾ Phase I

Most vendors support interoperable solutions for directory services and naming. While most directory data used today reside in integrated, vendor-proprietary messaging and file systems, the transition to an X.500 environment with access via the lightweight directory access protocol (LDAP) is the preferred implementation. As long as the back-end X.500 directory system is scalable, most systems that implement LDAP as the access technology are sufficient.

A new method of combining multiple directories, called meta-directories, is evolving. Meta-directories provide application-specific agents that synchronize the application directories (e-mail and operating systems) into a standard directory with access via the LDAP. LDAP has become a de facto standard as it is currently supported by most electronic messaging and Web-enabled applications.

4.6.4.1 Technology Policy

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

The DNS services will be located inside the SFA’s security firewall.

4.6.4.2 Standards

The SFA standard for naming services is DNS. Dynamic DNS is an emerging standard (RFC 2136) for dynamically making updates to the DNS when used in conjunction with other services such as the DHCP. 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.

4.6.4.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
DNS	TBD		

4.6.5 Remote Access Services

Remote access has become a strategic imperative for organizations worldwide. Remote access to enterprise information has become a strategic business asset, allowing many companies to securely distribute computing resources into the field. Remote clients have two methods of accessing local enterprise network resources: over the Public Switched Telephone Network



SFA Technology Policy Guide ¾ Phase I

(PSTN) or by “tunneling” through the Internet. Although tunneling will increasingly be used over time, access over the PSTN is the dominant connection method today worldwide.

The prevailing trend is to use “Remote Node” because it allows the 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. Once connected the remote client can download and upload files to reduce bandwidth charges by working off-line. 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.

4.6.5.1 Technology Policy

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.

4.6.5.2 Standards

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

4.6.5.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	Cisco 5300s	Cisco 5300s	Cisco 5300s
	Chatterbox/ PC Anywhere (migrating Citrix)	Chatterbox/ PC Anywhere (migrating Citrix)	Chatterbox/ PC Anywhere (migrating Citrix)
	Cisco Secure RADIUS	Cisco Secure RADIUS	Cisco Secure RADIUS

4.6.6 Virtual Private Network

A Virtual Private Network (VPN) is a private, secured network that exists within a public network and is 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 to provide 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. Tunneling is the act of encapsulating data within TCP/IP packets, using the Internet’s TCP/IP protocol. Many forms of Internet traffic currently use tunneling for information transfer, including FTP for file transfers and HTTP for information exchange



SFA Technology Policy Guide ¾ Phase I

between Web servers and browsers. Internet VPNs expand on this concept by providing data encryption and, in some cases, managing the stability and reliability of the network connection.

Although the cost savings can be considerable when compared to traditional VPN or WAN solutions, corporate VPNs over the Internet are not yet suitable in all situations or with all types of information. 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. Therefore, 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.

4.6.6.1 Technology Policy

TBD

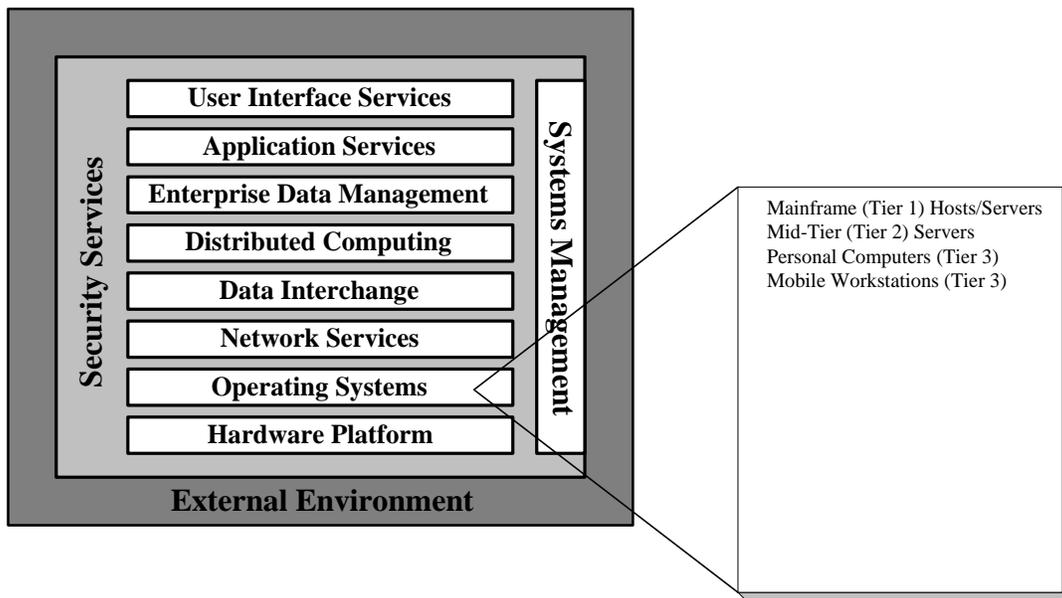
4.6.6.2 Standards

No published industry standard identified.

4.6.6.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	Under development		

4.7 Operating Systems



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:



SFA Technology Policy Guide ¾ Phase I

- 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.

4.7.1 Mainframe (Tier 1) Hosts/Servers

Operating system services provide the basic environment for running applications. These services consist of platforms and peripherals existing as nodes within a network. The mainframe host/server operating system will provide new ways of using existing data to achieve a competitive advantage. Customers will be able to 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 capability for handling large databases as a single image.

4.7.1.1 Technology Policy

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 is moving to the Parallel Sysplex technology configuration. SFA will select scalable servers that can increase performance by adding components and by supporting standards-based network protocols.

4.7.1.2 Standards

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



SFA Technology Policy Guide ¾ Phase I

4.7.1.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
OS/390	OS/390	OS/390	OS/390
CICS	CICS	CICS	CICS

4.7.2 Mid-Tier (Tier 2) Servers

Mid-tier operating system services provide the basic environment for running applications. (See the discussion on personal computer operating systems in Section 4.7.3.)

4.7.2.1 Technology Policy

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

Target Operating System	Function
Windows NT	Client/Server Applications Front End Communications
HP/UNIX	Client/Server Applications Host
Sun Solaris	Internet

4.7.2.2 Standards

Compliance with XPG 4.2 and POSIX standards allows for increased interoperability of hardware components and facilitates application portability. Typically the brand, such as XPG4 and UNIX 95, applies to a combination of platform and operating systems. For example, some XPG4-based, profile-branded platforms include HP-UX 9.X, running on HP 9000 series processors and UnixWare and later running on Intel platforms. SPEC 1170 is now included within the XPG 4.2 specifications. Although not XPG4 compliant, Windows NT is gaining major market share in the class of servers typically supporting large workgroups. 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.

The following table details the SFA standard configuration for the mid-range Hewlett Packard and Sun Solaris environments. The Windows NT environment will be deployed for processing the Micro Strategy suite of products.

4.7.2.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
HP/UX	HP/UX	HP/UX	HP/UX
Windows NT	Windows NT	Windows NT	Windows NT
	Sun Solaris	Sun Solaris	Sun Solaris



SFA Technology Policy Guide ¾ Phase I

4.7.3 Personal Computers (Tier 3)

Operating system services provide the user environment for running applications. These services consist of platforms and peripherals existing as nodes within a network. Traditionally, high-end workstations have been Reduced Instruction Set Computing (RISC)-based computers using a UNIX operating system. Today, however, workstations using Intel’s microprocessors running Microsoft NT 2000 Workstation are also being used in high-end computing applications such as application development, multimedia, and decision support data analysis presentation. NT 2000 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.

4.7.3.1 Technology Policy

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 for a preponderance of business applications on personal computers.

4.7.3.2 Standards

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.

4.7.3.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
Microsoft Windows 95	Microsoft Windows 2000	Microsoft Windows 2000	Microsoft Windows

4.7.4 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.)

4.7.4.1 Technology Policy

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.



SFA Technology Policy Guide ¾ Phase I

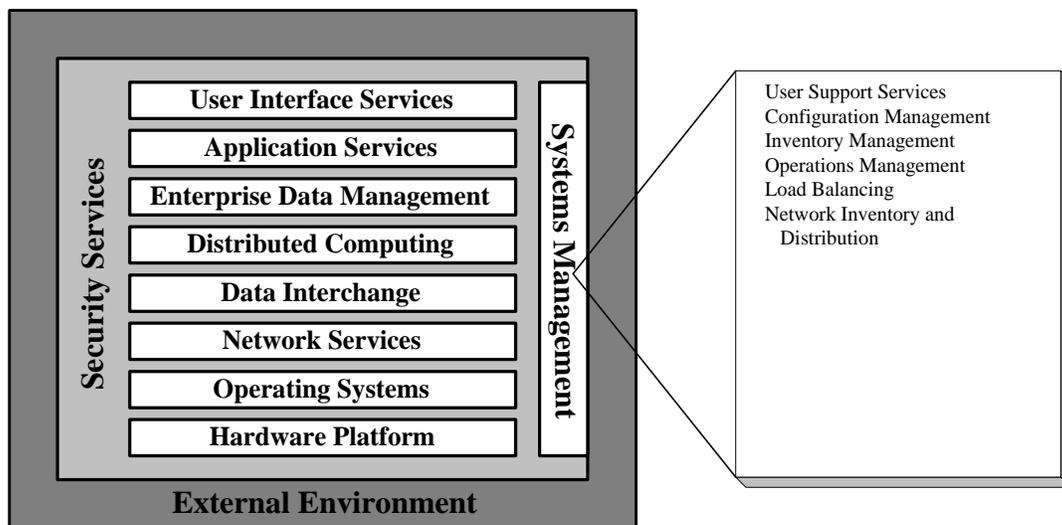
4.7.4.2 Standards

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.

4.7.4.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
Microsoft Windows 95	Microsoft Windows 2000	Microsoft Windows 2000	Microsoft Windows

4.8 Systems Management



The term 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 includes the following:

- Defining, resolving, and managing problems
- Operating networks and multi-vendor systems
- Distributing and managing software
- Operating information systems
- Planning and management performance
- Maintaining asset information (data)
- Developing short- and long-range IT plans
- Ensuring that IT goals and objectives are consistent with SFA goals and objectives



SFA Technology Policy Guide ¾ Phase I

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.

4.8.1 User Support Services

The user support services function 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.

4.8.1.1 Technology Policy

TBD

4.8.1.2 Standards

No published industry standard identified.

4.8.1.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TBD		

4.8.2 Configuration Management

Configuration management (CM) is concerned with maintaining, adding, and updating the relationships among components and the status of components themselves during system/network operation. The ultimate 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.

4.8.2.1 Technology Policy

TBD

4.8.2.2 Standards

No published industry standard identified.



SFA Technology Policy Guide ¾ Phase I

4.8.2.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
CCC/Harvest (Mainframe)	CCC/Harvest (Mainframe)	CCC/Harvest (Mainframe)	CCC/Harvest (Mainframe)
Computer Associates Endeavor (Mainframe)			
	Rational ClearCase (Non-mainframe)	Rational ClearCase (Non-mainframe)	Rational ClearCase (Non-mainframe)

4.8.3 Inventory Management

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. Automated products such as LANDesk can provide automated methods that can be used to obtain and maintain inventory information.

4.8.3.1 Technology Policy

To be identified.

4.8.3.2 Standards

To be identified.

4.8.3.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TBD		

4.8.4 Operations Management

The operations management function supports and controls the currently 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.



SFA Technology Policy Guide ¾ Phase I

- 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.

4.8.4.1 Technology Policy

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.

4.8.4.2 Standards

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.

4.8.4.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
Computer Associates CA-7 (Mainframe)			
BMC Control D (Mainframe)			
BMC Control M/R (Mainframe)			
Hewlett Packard OpenView (Mid-tier)			

4.8.5 Load Balancing

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.

4.8.5.1 Technology Policy

Load balancing 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



SFA Technology Policy Guide ¾ Phase I

- 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

4.8.5.2 Standards

No published industry standard identified.

4.8.5.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	IBM WebSphere Performance Pack	IBM WebSphere Performance Pack	IBM WebSphere Performance Pack

4.8.6 Network Inventory and Distribution

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.

4.8.6.1 Technology Policy

TBD

4.8.6.2 Standards

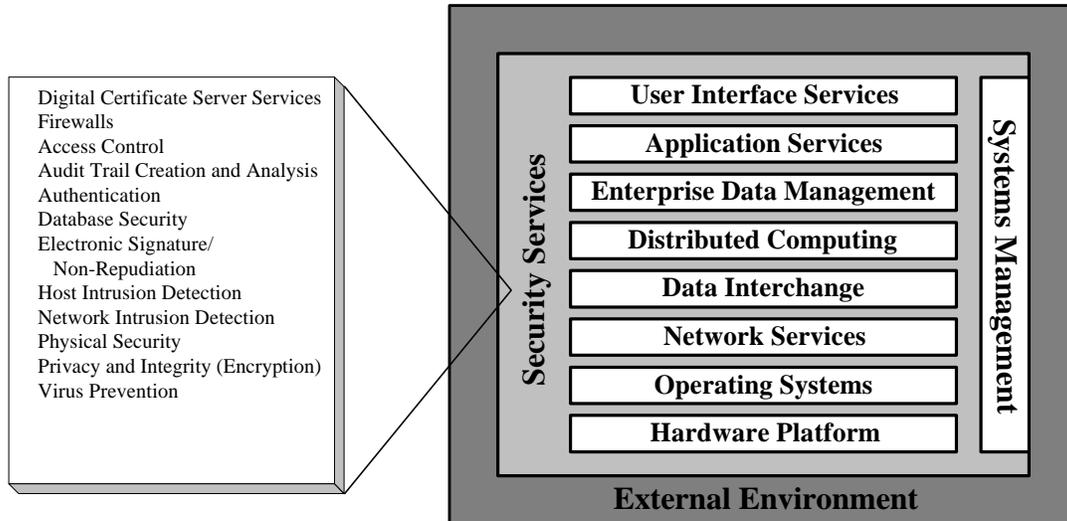
No published industry standard identified.

4.8.6.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	Microsoft Software Management System (SMS)	Microsoft Software Management System (SMS)	Microsoft Software Management System (SMS)



4.9 Security Services



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.

Two “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.

4.9.1 Digital Certificate Server Services

A digital certificate is a specially coded object that uniquely identifies a site. It 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



SFA Technology Policy Guide ¾ Phase I

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.

4.9.1.1 Technology Policy

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 must be able to handle large numbers of certificates and 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.

4.9.1.2 Standards

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.

4.9.1.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	Netscape Certificate Server	Netscape Certificate Server	Netscape Certificate Server

4.9.2 Firewalls

Firewall services protect sensitive information and resources that are attached to a network from unauthorized access. A firewall is a device that prevents the hazards of the Internet from extending to internal network; more specifically, it is a system that 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



SFA Technology Policy Guide ¾ Phase I

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).

4.9.2.1 Technology Policy

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.

4.9.2.2 Standards

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

4.9.2.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	CheckPoint Firewall-1	CheckPoint Firewall-1	CheckPoint Firewall-1

4.9.3 Access Control

Access control to data and applications is controlled 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



SFA Technology Policy Guide ¾ Phase I

individual applications. In the *n*-tier client/server computing environment, access control may be practiced at every tier.

4.9.3.1 Technology Policy

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.

4.9.3.2 Standards

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

4.9.3.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
RACF (Mainframe)	RACF (Mainframe)	RACF (Mainframe)	RACF (Mainframe)
Top Secret (Mainframe)			
BMC Control SA	BMC Control SA	BMC Control SA	BMC Control SA

4.9.4 Audit Trail Creation and Analysis

Audit trails 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



SFA Technology Policy Guide ¾ Phase I

4.9.4.1 Technology Policy

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.

4.9.4.2 Standards

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

4.9.4.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
RACF (Mainframe)	RACF (Mainframe)	RACF (Mainframe)	RACF (Mainframe)
	TBD (Mid-tier)	TBD (Mid-tier)	TBD (Mid-tier)

4.9.5 Authentication

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.

4.9.5.1 Technology Policy

Authentication must ensure that every subject or object using the system is identified that no methods exist to by pass identification. Identification must be enforced for both login sessions established through direct connected devices such as desktop workstations, and through remote devices, such as dial-up connections.

Authentication must manage some form of data that authenticates each subject or object of the system. The norm for a subject is a password, and a majority of systems are designed to deal with password authentication. 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 Technology Policy Guide ¾ Phase I

A legally meaningful warning message should be displayed during the login process that informs the user that the system is security aware. Such a message may contain a legal warning about use or misuse of the system.

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

4.9.5.2 Standards

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

4.9.5.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	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)

4.9.6 Database Security

Database management systems (DBMS) 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



SFA Technology Policy Guide ¾ Phase I

4.9.6.1 Technology Policy

The database maintains the user and user groups and controls permissions to 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.

4.9.6.2 Standards

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

4.9.6.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
RACF (Mainframe)	RACF (Mainframe)	RACF (Mainframe)	RACF (Mainframe)
Top Secret (Mainframe)			
	TBD (Mid-tier)	TBD (Mid-tier)	TBD (Mid-tier)

4.9.7 Electronic Signature/Non-Repudiation

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.

4.9.7.1 Technology Policy

TBD

4.9.7.2 Standards

TBD

4.9.7.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TBD		

4.9.8 Host Intrusion Detection

Host-based 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.



SFA Technology Policy Guide ¾ Phase I

4.9.8.1 Technology Policy

Now that the SFA is operating on Internet, computer systems and supporting technologies are at the heart of every organization. Data is very important, and if the integrity of that data is compromised, the entire organization could suffer. It could mean that SFA’s e-mail doesn’t work for an hour or it could mean that someone has gained access to confidential information.

SFA standard is that the tool for intrusion should be widely deployed and is 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.

4.9.8.2 Standards

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

4.9.8.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
Windows NT Tripwire	TBD	TBD	TBD
Sun Solaris Tripwire	TBD	TBD	TBD
HP-UX Tripwire	TBD	TBD	TBD

4.9.9 Network Intrusion Detection

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.

4.9.9.1 Technology Policy

TBD

4.9.9.2 Standards

No published industry standard identified.

4.9.9.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TBD		

4.9.10 Physical Security

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



SFA Technology Policy Guide ¾ Phase I

(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.

4.9.10.1 Technology Policy

TBD

4.9.10.2 Standards

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

4.9.10.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TBD		

4.9.11 Privacy and Integrity (Encryption)

Some information stored and routed on computer networks managed by SFA, privacy and integrity may be an important requirement. 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.

4.9.11.1 Technology Policy

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.



SFA Technology Policy Guide ¾ Phase I

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.

4.9.11.2 Standards

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

4.9.11.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TBD		

4.9.12 Virus Prevention

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. Numerous commercial products exist to provide virus prevention and detection in a variety of network environments. Products chosen should protect against the widest possible array of viruses, and should be compatible with the SFA’s architectures.

4.9.12.1 Technology Policy

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

4.9.12.2 Standards

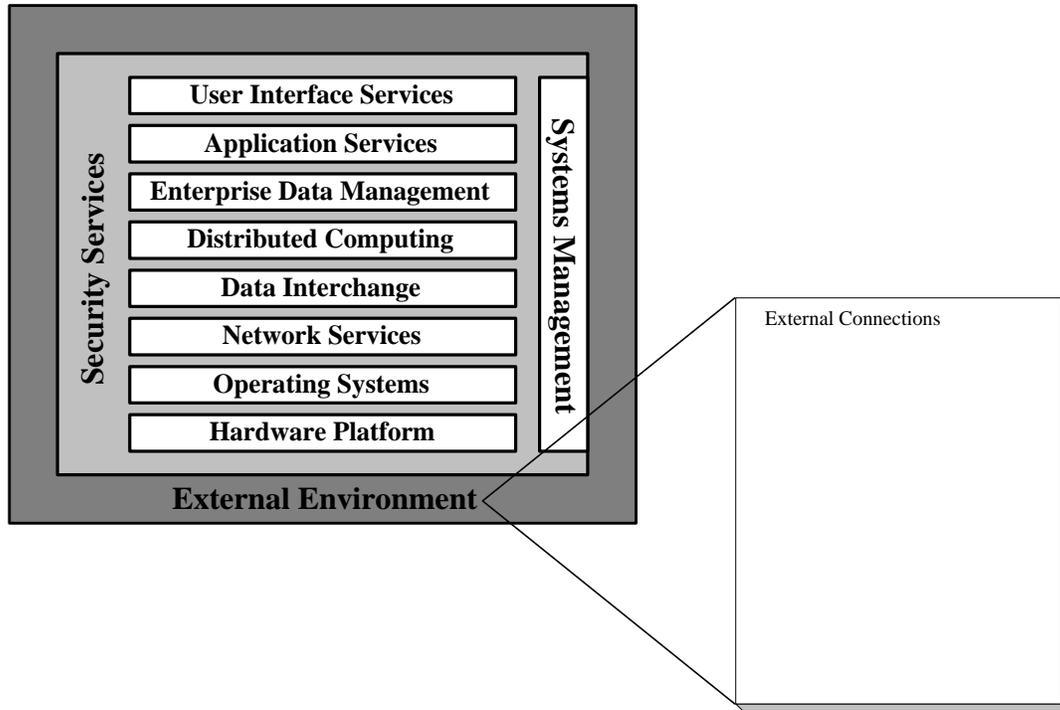
Relevant standards are identified in the Department of Education Security Policy and the evolving SFA Security Architecture.

4.9.12.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	McAfee	McAfee	McAfee
	Computer Associates Inoculan	Computer Associates Inoculan	Computer Associates Inoculan



4.10 External Environment



This section addresses external environment technologies and standards outside the scope of the TRM. The external environment addresses those technologies and standards extending beyond the physical and media access controls standards discussed previously. It encompasses issues involved with WAN and transmission systems not normally encountered by SFA personnel.

4.10.1 External Connections

WANs are divided into two parts. The first is defined as trunk technology and switching. For this part, the customer will generally purchase these services rather than invest in wide-area equipment and cable. The second addresses what the telephone industry refers to as the “local loop,” meaning the reach from the central office to the business or residence. In many cases, the customer may actually own such assets.

4.10.1.1 Technology Policy

The EDNet Metropolitan Area Network (MAN) consists of five major buildings: ROB3, FOB6, MES, 1990 K Street, and Capitol Place. These facilities are connected through Verizon’s Asynchronous Transfer Mode (ATM) network. ATM is provided to the buildings via a full-duplex 155 Mbps OC-3 link. The major MAN buildings are interconnected via ATM interfaces on Route Switch Modules (RSM), housed in Cisco Catalyst 5500s. For redundancy, the major facilities are also connected via Verizon’s Fiber Network Services (FNS), which provides 10



SFA Technology Policy Guide ¾ Phase I

Mbps connections. The FNS circuits are patched into a VLAN on the core Catalyst 5500 hub of each building.

EDNet's MAN has three minor buildings with FNS as their primary connectivity: Virginia Avenue, L'Enfant Plaza, and Portals. Cisco routers provide connectivity. These buildings have T-1 (1.54 Mbps) circuits connected to a Cisco 7206 router in ROB3 for redundancy.

There are four satellite offices in the EDNet MAN. They are connected via redundant T-1 circuits to Cisco 7206 routers within ROB3. The satellite offices consist of NAGB, NIFL, NEGP, and, Metro Center.

4.10.1.2 Standards

Relevant standards will be identified consistent with SFA's strategy to consolidate its WAN and further refinement of its Infrastructure Architecture, including the continued use of dedicated circuits and frame relay. Products are provided by commercial telecommunication services.

4.10.1.3 Target Standards and Timeframe

As Is	2000/2001	2001/2002	2002/2003
	TBD		



5 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



SFA Technology Policy Guide ¾ Phase I

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