

7. SECURITY ARCHITECTURE

IT Direction			
Business Architecture	Information Architecture	Application Architecture	Infrastructure Architecture
Security Architecture			
Enterprise Architecture Management (EAM)			

7.1 Overview

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.

The “Office of Student Financial Assistance Guide to Information Security and Privacy” document provides a view of the security technologies, policies and procedures to be implemented within SFA, giving the precise steps that should be implemented to reduce risk and ensure that SFA systems are available to SFA customers and partners in a timely manner. SFA security policies and procedures will be in conformance with the Department of Education guidelines as specified in “Information Technology Security Policy of the U.S. Department of Education.”

The SFA ITA will be designed to integrate security services across systems and platforms, covering all systems and applications. The “Integrated Technical Architecture Detailed Design Document, Volume 5, Security Architecture” and “SFA Information Security General Minimum Security Baseline Standards” (under development) detail the 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.

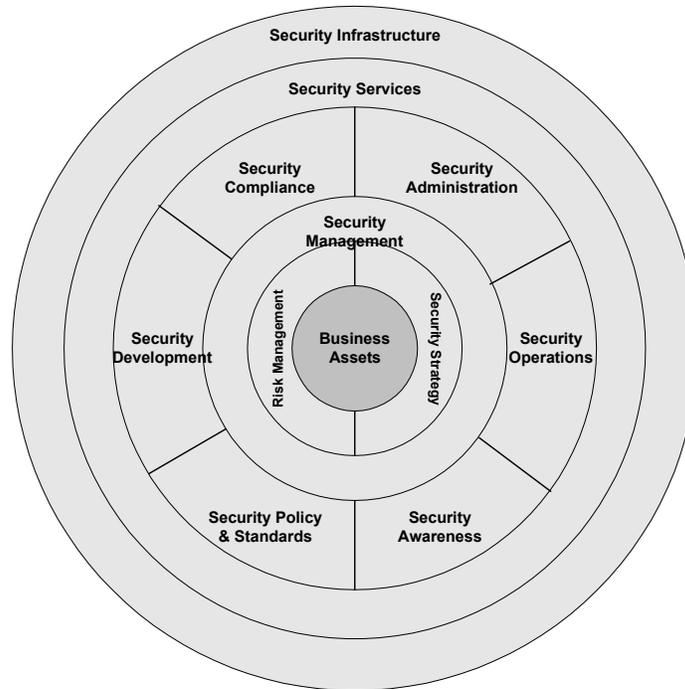
The goal of the SFA security operations is the safeguarding of assets while complying with all pertinent legislation and regulations.

7.2 Framework

The SFA program, as a key component of its modernization plan, is moving to provide its customers and partners high-speed, secure system access over the Internet. To make this happen, the architecture that supports this access must provide confidentiality, identification, authentication, authorization, data integrity, accountability and non-repudiation for all transactions.

Exhibit 7-1 below shows a conceptual view of the security architecture framework, with all functions focused on protection of the business assets.

Exhibit 7-1: Security Architecture Framework



The SFA Security Framework is a usable and comprehensive security overview. This Security Framework should be thought of as a conceptual structure used to frame the security-related technologies, systems and procedures to be designed and implemented. This Security Framework identifies what security components may be required and how the components fit together. Based on the inventory of components and the description of their relationships, the optimal solutions will be applied. The Security Framework comprises the following:

- **Business Assets**—represents what needs protection and the target of all information security efforts. The SFA Security Framework will contain all the necessary hardware and software to secure most SFA resources, including legacy applications (client/server and mainframe). It will furnish the necessary features that make the secure implementation of business functions and systems, such as virtual private networks, partners, E-commerce and customer and Internet lending-based systems, easier and less expensive.
- **Risk Management**—analyzes the business assets' value and the cost to protect the assets, identifies the level of protection required and discovers the threats and vulnerabilities that must be addressed through the security strategy. The discovery of threats and vulnerabilities is done through the monitoring and response to suspicious activity. The SFA Security Framework provides event monitoring and can detect multiple types of activities; detection occurs when someone tries to violate the system's security and allows the administrator to determine how to respond to the attempt. Each event's threshold is configurable for sensitivity before generating an alarm.

- Security Strategy—defines the approach and direction SFA is taking to secure and enable the business assets in line with the risk management approach. Within industry and government, most major systems development, communications and financial transactions are moving to the Internet. It is no longer enough to provide basic security commodity services (e.g., firewalls, secure routers and virus protection) that block and disable; it is also crucial to provide enabling services to all financial institutions, academic organizations and individual users so they can access SFA resources over the Internet securely. Therefore, the strategy of SFA security is to provide analysis of the commodity services employed at SFA, ensure network perimeters and devices are secure and then focus the emphasis on enabling technologies and solutions that support the SFA business model and drivers.
- Security Management—covers the overall responsibility for the management of the secure enterprise. Within this section, roles and responsibilities begin being identified. Central on-site and remote management capability is crucial for solving the network administration concerns of SFA. The configuration of remote sites from a centralized location provides an additional layer of administration and control of information security and, with the inclusion of strong authentication and virtual private networks, provides secure remote management. As with remote management, the delegated administration of users is crucial for solving the network administration concerns of SFA. Users inside and outside SFA can be delegated to their lowest common denominator, such as an academic financial administration group.
- Security Policy and Standards—aims to aid in achieving a secure environment by establishing consistency in architecture and to reducing the risk, effect and cost of security incidents. The SFA Security Framework will furnish centralized control for maintaining the SFA security policy and will deliver the flexibility for controlling and managing access through the Security Framework from a central location. These features include an easy to use management interface, configuration of remote sites and SNMP monitoring of all systems from a centralized location. The access control rules will shape the SFA corporate security policy. The SFA Security Framework will provide sophisticated access controls defined through measures such as time, day, user groups, network groups, network interface, inbound and outbound authentication and encrypted tunnels.
- Security Awareness—communicates the security policies and procedures to all employees, business partners and customers to establish SFA's expectations regarding information security and to communicate each individual's responsibility for protecting the confidentiality, integrity and availability of business assets. The objective of awareness is to ensure that a secure method of connectivity is provided between SFA and all locations, including third-party (partnering) companies and to provide a formalized method for the request, approval and tracking of such connections. The awareness programs and policy apply to all new connection and access requests and any existing third-party network connections. In cases where existing third-party network connections do not meet all of the guidelines and requirements outlined in this document, they will be re-engineered as needed.
- Security Compliance—includes all the functions that people perform to ensure that the Security Policy and Standards are created, followed, measured, enforced and updated as needed. The SFA Security Framework allows two levels of security precautions: It will protect the SFA Consumer Lending Intranet from intrusion and the combination of routers

and firewalls will check the source address of the Internet users that are attempting contact. The SFA Security Framework will provide fine-grained proxy services that will authenticate, authorize and control access to isolate activity between the two network interfaces, external and internal, by shutting off all direct communication between the two network interfaces. Network packets are never passed between these two interfaces.

- Security Administration—performs administrative processes, primarily oriented toward managing users throughout their life-cycle within the organization. The SFA Security Framework will utilize a GUI that allows for easy administration of access rules that define the security policy. Security administrators can set security parameters, control access and monitor activity through this interface. Access rules let the security administrator control connections based on time, day, user groups, network groups, network interface, inbound and outbound authentication and encrypted tunnels. To create a secure domain, all functions provided by the SFA Security Framework will administered via a common interface management console. This administrative interface will specify how the requesting user (no matter where located) will be allowed to participate in SFA secure domain. The SFA Security Framework will broker all the underlying network issues and security precautions to make the SFA Extranet, Intranet and Internet secure.
- Security Development—supports and enables the building of new security technologies, architectures, applications, systems and business capabilities as well as new security services and security infrastructure. The architecture will support application security, authorization and integration with WebSphere, Applets, Servlets, Enterprise Java Beans (EJB) components, CORBA, Java and legacy applications via standards and customizable application programming interfaces (APIs).
- Security Operations—responsible for the ongoing monitoring of security components and security events. The number and location of these Frameworks will be driven by business and institutional needs enabled by security, performance and quick reaction capability. If more than a single Framework is required, the directory structures for each Framework will be replicated to all other Frameworks. If any one Framework fails, for any reason, traffic will be routed to another Framework so that it can assume the failed Framework's responsibilities. Each Framework will be configured in a high availability configuration. This includes the deployment of redundant servers, RAID disk arrays, redundant Lightweight Directory Access Protocol (LDAP) directory structures and redundant communication paths. Where multiple Frameworks are being used to provide a common set of security services, the virtual aspect of Framework design can be used to balance the load across those diversely located SFA systems, thereby achieving better utilization of SFA resources and reducing capital investment.
- Security Services—supports reusable common security architecture components that have been documented and packaged to facilitate easy redeployment. The SFA Security Framework will offer security for the SFA Infrastructure. It will offer full security for all TCP/IP and legacy applications, presenting an implementation of a transparent gateway.
- Security Infrastructure—actual security components that provide protection for the business assets. The SFA Security Framework will contain all the underlying services responsible for ensuring a secure environment for Extranet, Internet and Intranet access, including single sign-on. Network and security mechanisms will include interaction with routers, firewalls and any necessary encryption functions. The SFA Security Framework will support a global

LDAP directory and registry function that will contain lists all the valid users, groups, organizations and password information necessary to provide inclusive single sign-on functions. The LDAP directory structure will contain an account entry for all valid security entities within a SFA domain. The SFA Security Framework will work directly in conjunction with the existing LDAP services supporting corporate email and DB2 systems supporting current user populations. The SFA Security Framework will allow for extensibility of services, to include integration with current network load balances, virtual private networks and token authenticators as well as future initiatives such as the GSA-ASIS Public Key Infrastructure project and Smartcard projects.

7.3 Components

Security is dependent on the policies, procedures and technologies used. This section describes the components of the SFA security architecture, including the functions, standards and policies. (For more detailed descriptions of these components, see Section 4.10, Security Services, of the "SFA Technology Policy and Standards Guide" [Appendix C in this document].)

7.3.1 Digital Certificate

Certificates may be implemented for individual users or for systems such as individual servers. Different classes of certificates can be generated with defined levels of trust. The highest levels of trust are typically used in financial transactions and where confidentiality requirements are high. Different types of certificates are required for specific cryptographic protocols such as SSL, S/MIME or IPSEC. The X.509 standards defines the data in a certificate. Certificates are commonly stored in a directory.

7.3.2 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. 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. 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.

7.3.3 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

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

7.3.4 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

When a security-relevant event occurs, the security audit service must generate an audit event that can be recorded, reported, archived and analyzed.

7.3.5 Identification and 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. 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.

7.3.6 Database Security

Databases maintain 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 and the database controls user accesses rights at each level. The provision of database management system security services includes data security policy management, data security service management, data security mechanism management and data security mechanism support management.

7.3.7 *Electronic Signature/Non-Repudiation*

Non-repudiation provides validation of the integrity and origination of electronically transmitted information. Digital signatures and file integrity checks may use strong encryption to protect data integrity and guarantee data authenticity with a reasonable degree of assurance.

7.3.8 *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. The system will identify what was changed and provide file names for a systems administrator to use for system restoration.

7.3.9 *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.

7.3.10 *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 (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.

7.3.11 *Privacy and Integrity (Encryption)*

For 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 on-line database access. Firewalls alone cannot protect such data outside the local perimeter.

Many forms of encryption software, based on various standards, are available. Two primary methods are Private Key Encryption and Public Key Encryption. The public key infrastructure (PKI) allows the method to be used widely. Any standards-based encryption is better than allowing the transmission of clear text across wide-area networks. The legal department and/or the appropriate government agency should be consulted any time encryption technology or encrypted information might cross government boundaries.

7.3.12 *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 e-mail attachments and file downloads. Incoming data

can be checked for harmful content at the public Inter-network boundary. Passive virus protection will be implemented throughout the network environment. SFA platforms will have current anti-virus software installed and active to scan memory, boot sectors, attachments and files.

7.4 Key Personnel and Roles

The effectiveness of SFA security will be dependent on personnel knowing and carrying out their security-related duties and obligations. The following people within SFA will have key roles in establishing and maintaining the security program:

- Chief Information Officer—responsible for ensuring full coordination of the security program, including between SFA and the Department of Education and between SFA and external agencies.
- Functional Managers—administratively and operationally responsible for computer systems within the channel, including responsibility for the establishment, maintenance and enforcement of the security policy.
- Computer Security Officer—responsible for the implementation and management of the security program within SFA, including being the point of contact for all security matters.
- System Security Officer—designated by Functional Managers to be responsible for the day-to-day security of that system, including implementing the security program as it applies to the system and the information within it.
- Users—responsible for being aware of and complying with security policies and procedures, including reporting security problems or incidents to the appropriate security officer.

7.5 Development and Implementation of Security Procedures

The development of the SFA security program will take place in a methodological approach. The following three steps comprise the approach:

- Risk Assessment/Gap Analysis
- Corrective Action Plan
- Implementation of the plan

7.5.1 Risk Assessment/Gap Analysis

Risk assessment/gap analysis reports are the first step in developing the SFA security program and ensure legislative compliance. A risk assessment/gap analysis has been conducted on the 11 systems identified by CIO Management as critical areas (see Section 7.6.4 below for a matrix showing the SFA applications/systems). The scores and results of these assessments are given in “Office of Student Financial Assistance Risk Assessment Report.”

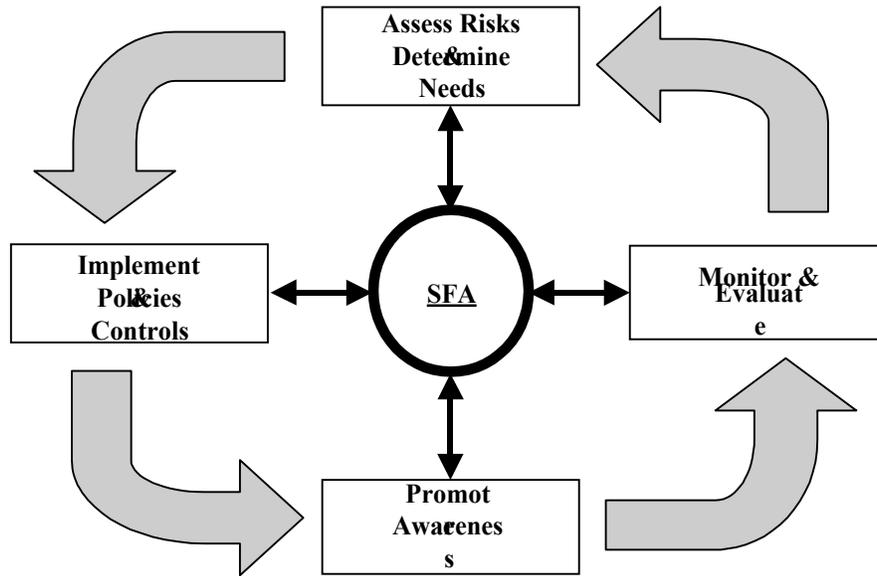
The SFA risk management methodology uses a four-step life-cycle maturity model, with actions and criteria defined at each step. The steps and their accompanying actions are:

- Assess Risks and Determine Needs

- General Description/Purpose
- System Environment
- System Interconnection/Information Sharing
- Applicable Laws or Regulations
- General Description of Information Sensitivity
- Risk Assessment and Management
- Review of Security Controls
- Implement Policies and Controls
 - Rules of Behavior
 - Security Life Cycle Planning
 - Authorize Processing
 - Personnel Security
 - Physical and Environmental Protection
 - Production, input/output Controls
 - Contingency Planning
 - Application Software Maintenance Controls
 - Data Integrity/Validation Controls
 - Documentation
 - Identification and Authentication
 - Logical Access Controls
 - Public Access Controls
- Promote Awareness
 - Security Awareness and Training
- Monitor and Evaluate
 - Audit Trails

Exhibit 7-2 below shows the SFA system risk management maturity overview, which emphasizes the continual review process. The assessment at each step feeds into the central focus point, which is the enterprise-wide security awareness encompassing a *point of contact*, a *plan* and a *strategy*.

Exhibit 7-2: Risk Management Maturity Overview



7.5.2 Corrective Action Plan

From the gap analysis, corrective action plans—detailing the specific steps needed to be performed to ensure security—will be developed for each system evaluated. Items within each corrective action plan will be prioritized based on critical need, as determined by CIO Management and security personnel.

7.5.3 Implementation of the Plan

Based on the corrective action plans and prioritization, the necessary technologies, policies and procedures will be implemented, with compliance and oversight by the business units and CIO staff.

7.5.4 Applications/Systems Matrix

Exhibit 7-3 below shows the status of the three steps.

Exhibit 7-3: Security Plan to Applications/Systems Matrix (September 2000)

	Application/System																					
	C B S	C D S	C P S	D C S	D L S	D L S	D L S	E D E x p r e s s	F A R S	F F E L P	F M S	G A P S	I F A P	M D E	N S L D S	P A S	P E P S	P M S	R F M I G	S S G	T I V W A N	
Risk Assessment/ Gap Analysis	C		C		C	C	C			C					C	C		C		C		C
Corrective Action Plan	U		U		U	U	U			U					U	U		U		U		U
Implementation	P		P		P	P	P			P					P	P		P		P		P

C = completed.

U = under development.

P = planned.

7.6 Minimum Security Baseline

A key methodology in the development of the SFA security infrastructure and accompanying plans and policies will be MSB. The MSB is designed to be used as a standard for implementing a minimum level of security on SFA information systems. MSB documents also detail the rules and processes for authentication, authorization, confidentiality, privacy, monitoring and data integrity controls. (See Appendix E in "Integrated Technical Architecture Detailed Design Document, Volume 5, Security Architecture," for the general MSB.)

7.7 Maintenance

The continuing effectiveness of the SFA security will depend on regular assessments and evaluations of all information systems. To this end, security checklists have been developed. (See Appendix C in "Integrated Technical Architecture Detailed Design Document, Volume 5, Security Architecture," for due diligence checklists.) Following the procedures outlined will ensure that all systems are in compliance with the SFA security program.

