

3	SECURITY REQUIREMENTS	3-1
3.1	Introduction.....	3-1
3.2	Information Systems Security Overview	3-2
3.2.1	Overview of Information Systems Security.....	3-2
3.2.2	Overview of Current SFA Systems Security	3-14
3.3	Security Requirements.....	3-16
3.3.1	Security Policy and Management Requirements.....	3-17
3.3.2	Physical Asset Security Requirements	3-19
3.3.3	User Types and Access Rights Requirements.....	3-26
3.3.4	User Authentication and Authorization Requirements	3-43
3.3.5	User Account Maintenance Requirements.....	3-53
3.3.6	Data Transportation and Encryption Security Requirements.....	3-55
3.3.7	System Security Auditing Requirements	3-66
3.3.8	Additional Topics	3-68
3.4	Security Awareness	3-82

3 SECURITY REQUIREMENTS

3.1 Introduction

Several major enterprise-wide modernization initiatives are currently planned within SFA. Security and privacy issues are a significant concern for ED and for the customers and partners whose contributions will be crucial to the success of these initiatives. There is currently no SFA-wide security policy or infrastructure to address these concerns.

This Section defines a uniform set of security requirements to form a basis for developing an SFA-wide security infrastructure. Adherence to these requirements will help ensure the confidentiality, integrity, and reliability of the systems using this infrastructure. Establishing these common requirements will reduce the costs associated with system implementation and maintenance by enforcing consistent standards among the systems. Consistent security guidelines are also necessary to protect customer interests and to thereby maintain customer confidence in the SFA environment.

This Section comprises the following subsections:

- **Subsection 3.2 Information Systems Security Overview.** This subsection provides an overview of information systems security mechanisms and reviews the current policies, procedures, and technologies utilized by SFA for the protection of data and system resources.
- **Subsection 3.3 Security Requirements.** This subsection defines specific security requirements for Project EASI/ED. Topics covered include Security Policy and Management, Physical Asset Security, User Types and Access Rights, User Authentication and Authorization, User Account Maintenance, Data Transportation and Encryption, System Security Auditing, and Additional Topics.
- **Subsection 3.4 Security Awareness.** A fundamental EASI/ED objective is to make information more readily accessible to a wide range of users. This objective increases the importance of organizational awareness of information security and of the need to ensure data confidentiality, integrity, and availability. This subsection presents a strategy for communicating information system security awareness to ED staff.

3.2 Information Systems Security Overview

This subsection provides an overview of existing industry security standards and practices and describes the current SFA system security environment. Subsection 3.2.1 describes information system security concepts, practices and industry standards; subsection 3.2.2 describes the current security environment in SFA.

3.2.1 Overview of Information Systems Security

Webster's New Riverside Dictionary (1996) contains the following definitions of the word "security":

- Freedom from risk or danger: safety
- Freedom from doubt, anxiety, or fear: confidence
- Measures designed to protect, as from theft, attack, or disclosure
- Written evidence of ownership or creditorship
- Something given to assure the fulfillment of an obligation pledge
- Prevention of the unauthorized use of a program or device

While the last of these definitions may appear the most appropriate in the context of information systems, enterprise-wide security infrastructure must consider facets of all these definitions. Users must feel confident that their data is safe from unauthorized modification, that their data cannot be stolen or improperly disclosed, that documents and transactions that are "signed" by an individual actually originate from that individual, and that other individuals cannot repudiate or deny a message that they send or a transaction that they authorize. SFA security must satisfy all of these requirements, but in addition it must ensure the maximum possible access to information for authorized users.

This subsection provides a picture of different mechanisms used to achieve security in information systems. It will provide ED and other members of the post-secondary education community with an understanding of the basic security requirements most IT systems should meet. The subsection begins with the different objectives of information system security. Subsection 3.2.1.1 describes the various mechanisms or practices which are used to achieve these objectives. Subsection 3.2.1.2 presents three scenarios to illustrate how these mechanisms come together to fulfill the aims of information systems security.

Information Systems Security Objectives

The four main objectives of information system security are:

- **Confidentiality.** Information will not be disclosed to unauthorized individuals or entities.
- **Integrity.** Information will not be altered from its intended state.
- **Availability Information.** Resources or the channels of communication for information exchange will be available to authorized users.

- **Non-repudiation.** All actions will be verifiable and will therefore not be subject to future repudiation by any of the parties involved in the transaction. In case of electronic transactions, it is all the more important to be able to prove that an action did take place.

The components for ensuring security with regards to achieving the above objectives are:

- Security Policy
- Authentication
- Authorization
- Administration
- Auditing
- Data Integrity

3.2.1.1 Security Practices and Mechanisms

Security Policy

Policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. The term policy is also used to refer to the specific security rules for particular systems. Additionally, policy may refer to entirely different matters, such as the specific managerial decisions setting an organization's e-mail privacy policy or fax security policy. The National Institute of Standards and Technology (NIST) Information Security handbook categorizes policies into three basic types:

- **Program policy** is used to create an organization's computer security program.
- **Issue-specific policies** address specific issues of concern to the organization, .e.g., e-mail security policy.
- **System-specific policies** focus on decisions taken by management to protect a particular system, . e.g., a policy for the National Student Loan Data System (NSLDS).

Authentication

Authentication is the verification of a user's claimed identity. Authentication tools provide the ability to determine the identity of a party to an interaction and to ensure that a message came from whom it claims to have come from.

This is important both when a user accesses a system as well as when two people are exchanging information. Authentication services ensure system entities (i.e., processes, hardware, and users) are uniquely identified. Thus, when a user accesses a system, or a message is received from a source, they both have to be identified as being bona-fide entities.

. Identification is the presentation of an identifier by the user requesting access. Next, the user's identification is authenticated. Authentication is the mechanism by which the system binds that identity to a real world entity and establishes the validity of this claim.

The authentication methods that validate this claim are based on something users know (such as a password), something users have (such as security tokens or smart cards), or something users are

(biometrics). Two-factor authentication - using two of the foregoing methods - provides a higher level of security than simple authentication.

Some of the major authentication mechanisms include:

- **Passwords.** Password systems work by requiring the user to enter a user identification (ID) and password (or pass phrase or personal identification number [PIN]) that only he or she knows. The system compares the password to a previously stored password for that user identification. If there is a match, the user is authenticated and granted access.
- **Security Tokens and Smart Cards.** Security token authentication systems combine something the user knows –(a PIN) and something the user possesses –(a security token resembling a credit card). The user enters a PIN, and if correct, the card generates a password, which the user enters manually via a keyboard. These are far more secure than passwords, but are more costly, difficult to administer and may require special equipment. There are no uniform standards in place for tokens. A smart card is similar to a token, however with smart cards put into a card reader the user may not have to enter a password.
- **Digital Signatures.** Digital signatures allow the receiver of a digitally signed electronic message to authenticate the sender and verify the integrity of the message. The sender electronically “signs” or scrambles the message using encryption. The message is decrypted or unscrambled by the recipient, thereby verifying that the message was sent by the stated sender.
- **Biometrics.** Biometric technology involves using a person’s unchanging physiological or behavioral characteristic, such as a fingerprint or voice pattern, to verify a person’s identity.

Single Sign On (SSO) is the ability to access multiple computer systems or networks after logging in once with a single authentication sequence. This is increasingly relevant in large, distributed Information System environments, like ED, where a number of different systems perform different functions. It is all the more important because the different, interacting systems may be of different types, vintages, and platforms. Since one of the concepts in the Project EASI vision is the ability of users to have one common interface to the system, giving them access to all the resources they need, an important requirement from any authentication service is the ability to provide SSO.

The type of authentication mechanism used for each situation will depend on the level of business risk associated with the situation. It also depends on the physical access method used. For example, a user accessing the system over the Internet faces a risk of compromise if they use a login-password mechanism without encryption.

Authorization

Authorization is the process of determining how an authenticated user is permitted to use specific system resources (e.g., data files, operator commands, input and output devices). An authorization mechanism automatically enforces management policies governing resource use.

The specific rules for authorizing access to resources enforce confidentiality and integrity by granting or denying access to read, modify, or create data records and by controlling the creation or deletion of resources

Administration

Administration is the process of defining, maintaining, and deleting user authorizations, resources, or the authorized privilege relationships between users and resources. Administration translates business policy decisions into a format that an information system can use. The resulting internal policy definitions can be enforced at the point of entry, at a client device, in network devices such as routers, and on servers and hosts. Security administration is an ongoing effort because business organizations, their systems, and their users are constantly changing.

Security monitoring provides a means of verifying that internal environment and firewall security is being implemented effectively, and alerts administrators of intrusion or suspicious events. Such reporting methods are usually rule-based and are defined by system security administrators. These rules define what to watch for and how to respond, if and when something goes wrong.

Auditing

Auditing is the process of data collection and analysis that allows system administrators, to verify that authentication and authorization rules are producing the intended results as defined in the enterprise business and security policy. Individual accountability for attempts to violate the intended policy depends on monitoring relevant security events, which results in a database of events (or audit trail) that can be analyzed to detect attempted or successful security violations. A record of events also needs to be maintained from the point of view of non-repudiation. This provides evidence that an exchange of information took place in the form claimed by any entity involved in the exchange.

Data Integrity

Data integrity refers to the requirement that data in a file remains unchanged or that any data received matches exactly what was sent. This includes accidental changes made to data while in a system or while transmission across a medium. It also encompasses error correction due to transmission losses.

Data integrity is ensured by a large number of different mechanisms and processes that work together. These include Error detection and Correction technologies, Cryptography, Authentication, Authorization and backup of critical systems.

Cryptography is the conversion of data into an unreadable form via an encryption algorithm and enables information to be sent across communication networks that are assumed to be insecure without losing confidentiality or integrity. Data confidentiality is achieved by encrypting the message at the sender and decrypting at the receiver. Encryption consists of transforming the message in such a way that only the intended recipient can interpret the message. Cryptography is also used for user authentication, as in the case of digital certificates.

An encryption algorithm transforms plain text into a coded equivalent, known as the cipher text, for transmission or storage. The coded text is subsequently decoded or decrypted at the receiving end and restored to plain text. The encryption algorithm uses a binary number key. The data is locked for sending by using the bits in the key to transform the data bits mathematically. At the receiving end, the key is used to unscramble the data, restoring it to its original binary form.

There are two primary types of encryption:

- **Private key encryption.** The same binary number is required to encrypt and decrypt the data. This single key must be kept secret for the information to remain secure; thus, a different shared key is required for each pair of users.
- **Public key encryption.** A cryptographic system that uses two keys - a public key known to everyone and a private or secret key known only to the recipient of the message. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know only the public key.

A public-key infrastructure (PKI) is the underlying technical and institutional framework that allows public-key encryption technology to be deployed widely. Technically, PKI refers to the technology, infrastructure, and practices needed to enable use of public-key encryption and/or digital signatures in distributed applications on a significant scale. The main function of PKI is to distribute public keys accurately and reliably to those needing to encrypt messages or verify digital signatures (used to sign transactions or to authenticate people prior to granting access to resources). This process employs digital certificates issued by an enterprise certification authority (CA) to users who register with that CA. Issuance of a certificate requires authentication of the user, usually by a registration authority (RA). The scope of PKI also extends to functions such as certificate renewal, certificate revocation/status checking, and user private key backup/recovery.

Supported applications could include secure e-mail, payment protocols, electronic checks, Electronic Data Interchange (EDI), IPsec network security, electronic forms, and digitally signed documents. Integral to a PKI are a means of authentication and encryption, secure directory services, secure interoperation of directory servers and client access to directories, and the Simple Distributed Security Infrastructure (SDSI).

3.2.1.2 Scenarios

Figure 3-1 presents a Project EASI/ED notional topology with the various security-related objectives and components illustrated. The following scenarios provide some representative examples of how these security components will work in the Project EASI/ED environment.

Scenario 1: School Account Creation

Figure 3-2 describes the process of a business partner such as a school creating a user account through Project EASI/ED. This scenario comprises the following steps:

Step 1: A school becomes an SFA partner and applies to the *Account Maintenance Service* for an Account for a particular user. The Account would consist of a suitable Identification mechanism like a digital certificate. The *Account Maintenance Service* would be accessible through the ED enterprise Directory Services. The school would have to apply through a secure medium, for instance a hardcopy application through facsimile.

Step 2: The *Account Maintenance Service* determines from the User Account policy rules that a School needs a Digital Certificate and sends a message to a *Registration Authority (RA)*

with the School details. This message is encrypted using the public key of the *Account Maintenance Service* while being sent to the *RA*.

Step 3: The *RA* collects information about the School and verifies user identity, which is then used to register a user according to the Account Registration Policy.

Step 4: The *RA* sends a message to the *Certificate Authority (CA)* who is responsible for creating, signing and issuing the certificate. The *CA* could be in-house or a third party. The information sent to the *CA* is encrypted using the *RA*'s private key.

Step 5: The *CA* receives the message and creates a *Digital Certificate* for the particular school representative, which may include a validation period and a timestamp, and lodges it in the *Certificate Repository*.

Step 6: The *CA* sends certificate information back to the *Account Maintenance Service*. All these communications are encrypted using the *CA*'s private key.

Step 7: The *Account Maintenance Service* accords the necessary user access rights to the school representative, according to the user access rights policy and creates the entries in the access control database, and makes necessary entries in the Access Control Lists (ACL).

Step 8: The *Account Maintenance Service* sends an encrypted message to the School Representative, with the confirmation about the creation of the account.

Notes:

All communications are encrypted using public key encryption.

All communications between the ED enterprise network and public networks will pass through the ED network firewall.

The *Account Maintenance Service*, the *RA*, and the *CA* are all part of an enterprise wide Directory Server.

Scenario 2: School representative performs financial transaction

Figure 3-3 describes a financial transaction between a School Representative and SFA. This scenario comprises the following steps:

Step 1: The school representative authenticates himself to the *Authentication Service (AS)* using his digital certificate. He accesses the SFA AS over the web, using a protocol like Secure Sockets Layer (SSL).

Step 2: The *AS* decrypts the digital certificate information (using the *CA*'s key and the *AS* key) and verifies the information against the *CR* on the directory server.

Step 3: If the information is accurate, the school representative is sent a message accepting the Authentication request, and the *AS* issues the school representative with a ticket allowing him to access the SFA systems. Otherwise, the request is rejected and appropriate action taken.

Step 4: The school representative has access to the SFA systems using the SSO ticket and his digital certificates. He issues a transaction request to the appropriate subsystem. The

subsystem authenticates the school representative against the ticket and the Digital Certificate, checking the Certificate repository, and grants or rejects the request.

Step 5: The school representative is authorized to perform the transaction, by the *Authorization Service*.

Step 6: The subsystem takes the information supplied by the transaction request from the school representative and processes it, talking to the database server, with the subsystem and the database mutually authenticating themselves.

Step 7: The subsystem sends back the result of the processing to the school representative in an encrypted form.

Notes:

All communications are encrypted using public key encryption.

All communications between the ED enterprise network and public networks will pass through the ED network firewall.

The *Account Maintenance Service*, the RA, and the CA are all part of an enterprise wide Directory Server.

Scenario 3: New student account and transaction over the Web

Figure 3-4 describes Internet-based transactions between the student and components of the system. This scenario comprises the following steps:

Step 1: The student submits a request for an account via the Web.

Step 2: The request is received by the authorization service. An account is created for the student.

Step 3: The authorization determines the access rights that the student will have by checking the appropriate access levels for a new student account in the access rights database.

Step 4: The student's new ID is sent to the student via the Web.

Step 5: The student submits a change of address request, which is routed to the appropriate application server and database by directory services.

Step 6: The application receives and updates the information.

Step 7: Confirmation of the change of address is sent to the student via the Web.

Notes:

All communications are encrypted using public key encryption.

All communications between the ED enterprise network and public networks will pass through the ED network firewall.

The *Account Maintenance Service*, the RA, and the CA are all part of an enterprise wide Directory Server.

3.2.2 Overview of Current SFA Systems Security

The current SFA systems conform to ED guidelines, including the Department of Education ADP Security Manual. However, each system has its own security technology, with little connectivity between different security systems. This situation is compounded by the fact that the systems are of different vintages and work under different operating environments.

An important aspect of the Project EASI vision is to provide a single point of interface to all systems that a user needs. If a user accesses multiple systems in the course of a single business process, he or she should be authenticated once to the entire system, rather than separately on different systems. Therefore, there is a crucial need for SSO capability encompassing all the interconnected systems that a user interacts with. At present SFA systems do not have this capability.

Most of the current SFA systems have multiple levels of security:

Operating System Security

Security is controlled by the operating system (OS). The OS maintains a list of users, groups, and privileges. The OS authenticates users when they log in using a mechanism like a user name and password. The users have a unique ID and have specific privileges relating to resources controlled by the OS, such as the file system, printers, and other system wide objects. This is usually the front line point of entry into any system.

Database Security

The database maintains the users 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. Databases control user access rights at each level (table, field and row). Row level access is usually controlled through views.

For example, the PEPS database environment is Oracle, which maintains users and groups. Oracle controls access to rows based upon database views.

Application Specific Security

Most applications have a set of business rules, which govern what different users can do in the application. These are controlled through various mechanisms, the most common being the user interfaces that a user sees or can use. For example, a user may see a menu with only those actions enabled that are permitted by his or her identity and profile. The application may maintain its own list of users and groups or may interface with other levels of security to determine these.

Dedicated Security Applications

There are security management applications like Resource Access Control Facility (RACF) in IBM environments, which manages security across the application. This interacts with other levels of security, i.e., the database, OS and application.

For example in NSLDS, IBM RACF authenticates a user based on user IDs and passwords and user groups. DB2 communicates with RACF to determine a user's ID and group, which corresponds to DB2 primary and secondary IDs, and uses them to allow or deny privileges to database objects. Here RACF is responsible for identification and authentication, but DB2 controls authorization to access database resources.

There are two initiatives at ED that share security services across SFA systems. They are the Title IV Wide Area Network (WAN) and the Education PIN (ePIN), which is a common authentication mechanism for access to systems over the Internet. It is currently used for FAFSA on the Web and NSLDS.

Title IV WAN Security

The Title IV Wide Area Network (WAN) connects various ED partners including schools and lenders, and various SFA systems like NSLDS, CPS, LOS, RFMS, CBS, and FFEL.

The Title IV WAN provides the authentication functions for office automation, electronic mail, and other enterprise wide utilities. Authentication is through a user name and password mechanism. The system protects access to the file system, protecting the network wide data and files. In addition, authorization and access control to the file system are maintained on a user by user basis. Each individual has a unique ID, which can be linked to editable actions taken by that user. Non-routine occurrences that may indicate a security violation generate audit trails.

ED is currently pursuing a Virtual Private Network (VPN) solution that will include PKI capabilities.

Education PIN

The ePIN or Electronic Access Code (EAC) serves as a unique identifier to let students access their personal information in various ED systems over the Web. Currently, it is being used on the NSLDS web site, FAFSA on the web, and is soon to be deployed on the Direct Loan Servicing web site. The ePIN is like the PIN that people receive from their bank in order to access their accounts through an ATM machine. The ePIN is generated from the user's Social Security Number, the first two letters of the user's last name, and the user's date of birth. The ePIN will be used as the PIN for Access America for Students Student Account Manager (SAM) Website.

3.3 Security Requirements

The following subsections document and define security requirements for Project EASI/ED:

- 3.3.1 Security Policy and Management
- 3.3.2 Physical Asset Security
- 3.3.3 User Types and Access Rights
- 3.3.4 User Authentication and Authorization
- 3.3.5 User Account Maintenance
- 3.3.6 Data Transportation and Encryption
- 3.3.7 System Security Auditing
- 3.3.8 Additional Topics

Each subsection contains a description of the security area to which the requirements in that subsection pertain, general requirements related to the security area, and then specific requirements related to particular topics within the area. If there are major developments in industry or technology, or specific issues relevant to SFA that relate to the area, these are discussed as issues and strategic findings. The subsection concludes with a discussion of representative standards and products.

Requirements are numbered using the numbering convention defined in the *Project EASI/ED Business Area Requirements Document (BARD) Version 2.0, August 17, 1998*.

3.3.1 Security Policy and Management Requirements

Consistent security policy and management are necessary to ensure that all Project EASI/ED requirements are implemented and managed in the same manner. This subsection will document the required elements of a security policy to be followed by organizations implementing Project EASI/ED systems. The subsection will introduce the purposes of having a system security plan and then list the elements that such a plan should contain.

Description: The purposes of a system security policy are to:

- provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements; and
- delineate responsibilities and expected behavior of all individuals who access the system.

A system security management policy documents the rules of managing the system. It defines security-related issues that must be addressed during the design, implementation, and maintenance of the system. Such a policy ensures that information in the system is secure at all times and creates a foundation for internal control of the system.

A system security management policy must be in place to ensure that the means of addressing these issues are readily available to the personnel who will build, maintain, and manage the system.

**General
Security Policy
Requirements:**

- 6500 Security management policies must be documented.
- 6501 Operations policies must be documented.
- 6502 Disaster contingency planning and recovery policies must be documented.
- 6503 Physical security policies must be documented.
- 6504 Problem management policies must be documented.
- 6505 Change management policies must be documented.
- 6506 System security controls policies must be documented.
- 6507 System development controls policies must be documented.
- 6508 Communications controls policies must be documented.
- 6509 Personnel controls policies must be documented.
- 6510 Asset classification policies must be documented.
- 6511 Compliance policies must be documented.
- 6512 A standard privacy policy statement must be created that defines what information is to be collected from individuals and how that information will be used.
- 6513 Guidelines for administering system security must be defined, including the classification of security personnel.

**General
Security**

Management Requirements:

- 6514 Relevant federal guidelines which impact the construction and use of the system must be documented.
- 6515 Access rules for system administration and users must be documented based upon the type of user. This section must define the user groups within the system and rules governing the creation of new users.
- 6516 There must be a policy governing the integration of security mechanisms between different systems.
- 6517 Software security must be reviewed when software is implemented or upgraded. Additionally, periodic software security reviews must be conducted.
- 6518 Rules for managing the relationship with contractors who build or maintain the system are documented in this section.
- 6519 General business objectives must be documented.
- 6520 Organization of security staff must be documented.
- 6521 Responsibilities of security staff must be documented.
- 6522 Segregation of duties of security staff must be documented.

Operations and System Administration Requirements:

- 6523 Systems software policies must be documented.
- 6524 Technical support contacts and policies must be documented.
- 6525 Hardware management policies must be documented.
- 6526 Data management policies must be documented.
- 6527 Documentation policies must be documented.
- 6528 System logs policies must be documented.
- 6529 Job scheduling policies must be documented.
- 6530 Utility policies must be documented.
- 6531 Printed reports policies must be documented.
- 6532 Problem reporting policies must be documented.
- 6533 System management reporting policies must be documented.

3.3.2 Physical Asset Security Requirements

This subsection documents requirements for securing the physical asset components of the EASI/ED system. Physical asset security is fundamental to protecting the system because without meeting physical asset security requirements, the confidentiality and integrity of information may be compromised by intentional destruction or by accident. Furthermore, availability of information may be lost due to natural or man-made events if the hardware used to store and to present the information is not secure. This subsection will present an introduction to physical security concepts, followed by specific Project EASI/ED physical security requirements.

Description: Physical security is the most basic and commonly addressed form of data processing control. Sensitive areas include computer operations, general work areas and areas housing essential support systems such as air conditioning, communications equipment, power supplies, cabling, power control panels and tape or disk storage areas.

The degree of precaution that should be taken to minimize these risks should be based upon the value of the data being accessed and the possibility that unauthorized access or a disaster could occur.

Good physical security planning includes consideration of threats to the computer site from natural disasters, human error, computer hackers, accidents, vandalism, electronic eavesdropping and theft.

Physical security concerns itself with the prevention of unauthorized physical access to a site and the implementation of security devices and procedures to prevent disaster or damage to the computing environment.

The three basic areas of potential vulnerability under the umbrella of physical security are:

- Physical access
- Environmental hazards
- Fire and flood protection

Physical Access

The controls over physical access should be reviewed to ensure that only authorized individuals are allowed access to the installation under appropriate management review and supervision.

There are four major areas of concern:

1. **Location of Sensitive Areas:** A list should be compiled of all potentially vulnerable areas, including their location and use and their position relative to other tenants in a building. Sensitive areas should be identified and perimeter controls should be in place.
2. **Entry and Exit Point Identification and Control:** Entry and exit points to all sensitive areas should be identified, including potential access points

such as air conditioning vents. Unnecessary doors or windows should be noted, as well as fire exits. Access point controls should also be assessed, including entry/exit logs and electronic and visual surveillance equipment, within the organization and externally in cases where building access cannot be restricted.

3. **Access Authorization Procedures and Monitoring Devices:** Some procedural concerns are addressed in Security Policies and Management, such as immediate notification to the appropriate departments of termination of a staff member's employment. Access authorization procedures should be used for all persons requiring access to sensitive areas such as employees, contract workers, security staff and visitors. Specific access procedures may include, granting and discontinuing of authorizations, control over passkeys, re-entry procedures after emergencies, controls over entry by time of day and reception area policies. There is a broad range of personal monitoring devices, from photo ID badges to smart cards. The monitoring systems may include such features as multilevel access or anti-passback. A review of the appropriateness of such monitoring devices and recommendations for changes or upgrades when necessary should be part of the physical security review.
4. **Audible and Silent Alarms:** Alarms should be fitted to all entry and exit points in sensitive areas. In organizations where on-premise security personnel are not present 24 hours a day, a schedule of "on-duty" executive level personnel may be required to ensure appropriate security precautions are taken in the case of an out of hours alarm. All alarms and other electronically-controlled security devices should be connected to a back-up power source to allow them to remain functional in the event of a power failure.

Environmental Hazards

Environmental hazards refer to the physical environment and the specific business environment. They include both natural and man-made hazards. Fire and flood, the two major causes of physical damage to data, are addressed as a separate topic.

The environmental hazards that should be assessed include:

1. **Assessment of Nearby Businesses:** The location of the organization as well as the specific location of the data processing areas should be assessed to determine proximity to businesses posing potential hazards such as oil refineries and chemical manufacturers. Potential internal hazards such as gas boilers, oil tanks and paper stores should also be noted;
2. **Areas Prone to Natural Disasters:** In areas prone to natural disasters such as earthquakes, tornadoes or floods, a physical security review should include a more detailed review of appropriate procedures and local building ordinances concerning disaster-resistant building standards.
3. **Electrical Supply:** This assessment should include a review of alternative

power suppliers such as motor or battery generators or an alternate electricity substation. A reliable source of back-up power should always be available. Power regulation systems should also be reviewed, including voltage regulators or uninterruptible power supplies (UPS). The effects of a power failure on the computer and on essential support systems such as air conditioning, humidifiers, alarm systems, access control mechanisms and lighting should also be assessed.

4. **Specific Data Processing Environment:** Each data processing area should be assessed for potential threats from heat and direct sunlight, dust, static electricity and humidity. Excessive dust levels or poor air filtration can cause computers, printers or other peripherals to fail more frequently. High relative humidity levels (i.e., 80% and above) can cause problems in computer systems including the corrosion of electrical contacts or the expansion of paper.
5. **Low Relative Humidity:** Low humidity can allow charges of static electricity to build up, causing paper to stick and jam. If this build-up discharges, it can damage magnetic devices such as tapes and disks.
6. **Air Conditioning and Temperature Regulation:** Temperature regulation is an essential support mechanism for all computer and data processing areas. These facilities should be reviewed for adequacy and the maintenance schedules should be adhered to.
7. **Man-Made Threats:** Some organizations may be more susceptible to terrorist threats or strikes and this risk should be evaluated. Procedures should be in place to manage such situations, both to attempt to stop them, as well as manage their aftermath, should they occur.
8. **Industrial Espionage:** Electromagnetic or radio frequency emissions could be intercepted by third parties and used to obtain information. This risk was formerly a preoccupation of the defense industry, but increasingly other organizations are becoming aware of it. The major control against this risk is the use of Tempest facilities (Transient Electromagnetic Pulse Emanations Standard) and involves the introduction of a Faraday cage to shield sensitive equipment. Similar measures may also be necessary to prevent radio interference at computer installations situated near airports, sea ports or military installations.

Fire and Flood Protection

Fire and flood, along with the resultant damage caused by fire extinguishing procedures (such as smoke and water damage) are two of the most common causes of damage to data processing equipment and records.

There are two major areas of concern:

1. **Flooding:** Flooding most often occurs through breakage of cooling or drainage pipes located in computer room ceilings, walls or floors. Water and drainage pipes should be routed away from computer operations areas. Additionally, an assessment should consider the potential for water storage

tanks to flood computer areas, the location of shut-off valves and moisture-detection equipment and the susceptibility to external flooding; and

2. **Extinguishing Equipment:** Detection and automatic extinguishing equipment should be reviewed for adequacy as well as documented records of regular, ongoing testing and maintenance of equipment and testing of evacuation procedures.

There are a number of fire-extinguishing systems available and both hand-held and automatic systems should be checked to verify the appropriate type is being used in each instance. Dry chemical portable extinguishers should never be used around computers as their corrosive agents can damage electronic equipment and data storage materials. The most popular and least damaging extinguishing compound for use in a computer environment is a gas called Halon 1301, although Halon is now considered to be hazardous to the ozone layer. Many organizations are now looking to use a Halon substitute, to return to water-based systems or to implement Halon recycling systems. In these situations, it is best to use a "dry" system where water is not held in the pipes but is released when a fire is detected.

As mentioned, a physical security review should include potential threats posed by adjacent buildings (or businesses within a multi-tenanted building), particularly if such areas are outside the organization control. Procedures for extinguishing fires in such areas should also be reviewed.

**Inventory
Documentation
Requirements:**

- 6600 Inventory documentation should include a description for all major equipment and items, including age, model and serial numbers and quantity of equipment.
- 6601 Inventory documentation should include information on the physical location of equipment.
- 6602 Inventory documentation should include details of the individual or department responsible for equipment.
- 6603 Inventory documentation should include supplier contact details.
- 6604 Inventory documentation should include financial information (e.g., cost and depreciation schedule).

**Entry Point
Requirements:**

- 6605 Facilities entry point access controls such as pass keys or electronic locking systems must be in place.
- 6606 After hours access to the facilities must be limited.
- 6607 Facility windows must be minimized, where applicable
- 6608 Unnecessary doors at the facility must be removed, where applicable.
- 6609 Fire exits at all facility entry/exit points must be fitted with panic opening devices.
- 6610 Entry points such as air conditioning ducts or vents must be noted.
- 6611 Wherever possible, equipment must not be located near exits.
- 6612 Emergency power-off switches must exist and be sited near exits at the

		facilities.	
Access Authorization Procedure Requirements:	6613	Perimeter controls must be in place segregating other tenants in multi-tenanted building facilities.	
	6614	Documented procedures should exist for granting and removing access authorizations.	
	6615	Documented procedures should exist for notification of users who leave or whose employment is terminated.	
	6616	Documented procedures should exist for control over distribution of pass keys and access cards for all employees including contract employees, cleaning staff and security personnel.	
	6617	Documented procedures should exist for re-entry procedures after emergencies.	
	6618	Documented procedures should exist for controls over entry by time of day.	
	6619	Documented procedures should exist for reception area policies including issue and return of visitors' access cards.	
	6620	Documented procedures should exist for audit of ability to access the computer areas.	
	Identification Badge Requirements:	6621	Color of the identification badge must be used to differentiate access levels.
		6622	A photograph of the employee must be on the identification badge.
6623		There should be a protocol to challenge staff who are not wearing appropriate identification badges.	
Electronic Security Systems Requirements:	6624	Electronic intrusion detectors covering all data processing areas should exist.	
	6625	Electronic vibration or transient sensors must be placed on windows, frames, fire and access doors and service ducts.	
	6626	Electronic security movement detectors covering areas of high sensitivity (such as tape libraries) must be used.	
	6627	Electronic security sensor communication must be protected from fire, flood and sabotage.	
	6628	Audible and silent alarms, locations and method of operation such as "fail open" controls must exist.	
	6629	Tamper proof power supply for access control system must be implemented.	
	6630	Surveillance systems (closed circuit television) equipment must be used to monitor entry/exit points and sensitive equipment locations.	
Access Control Requirements:	6631	Appropriate control over microcomputers and their peripherals access must exist.	
	6632	Appropriate control over workstations/terminals access must exist.	
	6633	Appropriate control over printers access must exist.	
	6634	Appropriate control over Local Area Network (LAN)/ Wide Area Network	

		(WAN) servers and other types of servers must exist.
	6635	Appropriate control over point-of-sale terminals/scanners must exist.
	6636	Appropriate control over tape and disk libraries and storage safes must exist.
	6637	Appropriate control over hand-held or laptop computers must exist.
	6638	Appropriate control over all other related devices must exist.
	6639	Appropriate control over negotiable and sensitive documents (checks/bonds/policy documents) must exist.
	6640	Appropriate control over remote controllers, cable panels and also the switchboard (e.g., Public Branch Exchange [PBX]) areas must exist.
Disposal Control Requirements:	6641	Controls must exist for disposal of input documents.
	6642	Controls must exist for disposal of paper outputs.
	6643	Controls must exist for disposal of magnetic material.
	6644	Controls must exist for disposal of printer ribbons and cartridges.
	6645	Ensure that all electronic media (e.g., disk drives) be cleared or destroyed.
Nearby Business and Location Evaluation Requirements:	6646	Identify nearby business with potential hazards such as oil refineries and chemical manufacturers.
	6647	Location of internal building hazards such as gas boilers, oil tanks and paper stores must be documented.
	6648	The physical location of the computer equipment, e.g., the computer room should not be a glass-walled room on the ground floor open to public view.
Evaluation of the Susceptibility of the Location to Natural Disasters Requirements:	6649	Susceptibility of the location to natural disasters such as earthquakes, tornadoes, hurricanes and flood plains should be evaluated.
	6650	Local building ordinances concerning disaster-resistant building standards must be evaluated.
	6651	Susceptibility of the location to vehicle impact should be evaluated.
Provisions for Continuous Electrical Power Regular Testing Requirements:	6652	Provisions for continuous electrical power should include the provision of the connection to alternative electricity substation.
	6653	Voltage regulators must be used to protect against power fluctuations.
	6654	Motor or battery generator for alternative power and uninterruptible power supplies must be used.
Evaluate Specific Threats Data Processing Sites Requirements:	6655	Evaluate specific threats to each data processing site resulting from cold, heat and direct sunlight and other temperature extremes.
	6656	Evaluate specific threats to each data processing site resulting from dirt and dust – especially for printers.
	6657	Evaluate specific threats to each data processing site resulting from static electricity.
	6658	Evaluate specific threats to each data processing site resulting from

ineffective air conditioning systems including humidity controls.

- 6659 Evaluate specific threats to each data processing site resulting from smoke or other types of air pollution.
- 6660 Evaluate specific threats to each data processing site resulting from electrical noise.
- 6661 Evaluate specific threats to each data processing site resulting from chemicals or solvents.
- 6662 Evaluate specific threats to each data processing site resulting from vermin/insects.
- 6663 Evaluate specific threats to each data processing site resulting from lightning.
- 6664 Evaluate specific threats to each data processing site resulting from vibration.
- 6665 Evaluate specific threats to each data processing site resulting from humidity.
- 6666 Evaluate specific threats to each data processing site resulting from water.
- 6667 Evaluate specific threats to each data processing site resulting from radio transmissions.
- 6668 Evaluate specific threats to each data processing site resulting from power level fluctuations.
- 6669 Fire and flood protection requirements will include evaluation that water pipes and drains are appropriately routed.
- 6670 Fire and flood protection requirements will include evaluation that the facilities are not be susceptible to external flooding.
- 6671 Fire retardant materials must be used for internal walls, partitions, and doors.
- 6672 Adequate fire and smoke detection equipment must be installed and tested.
- 6673 Automatic fire extinguishing equipment must be installed and tested.
- 6674 Adequate fire resistant storage facilities must be installed.

**Fire and Flood
Protection
Requirements:**

**Issues and
Strategic
Findings:**

All IT assets are in the process of being co-located at the Computer Sciences Corporation (CSC) Data Center at Meriden, Connecticut. Therefore, all physical access requirements will primarily apply to that facility, and may require modification depending upon particular circumstances that exist at Meriden.

3.3.3 User Types and Access Rights Requirements

This subsection defines the level of access that different users within the EASI/ED system will have to the system data, and indicate their ability to create, read, and update each type of data. This subsection defines a set of Project EASI/ED user types and documents functional access, stating the level of access appropriate for each user type to the data defined in the *Project EASI/ED Logical Data Model Document (LDMD) Version 2.0*, October 20, 1998.

The Privacy Act requires ED to protect the privacy of the individual participant information that forms the core data in the SFA student financial aid systems. ED also must ensure the protection of business-sensitive data relating to the various postsecondary education community organizations (e.g., schools, lenders, guarantors, secondary markets, servicers). In addition, ED must adequately secure data and transmissions, while maximizing data access by a large and diverse user community.

To facilitate the review of Project EASI/ED data access security, the Project EASI/ED data was further categorized into 14 major areas (as defined in the *Project EASI/ED LDMD*). A more detailed definition of these subject areas, based upon previous Project EASI/ED work, is detailed in Appendix E. The following table shows the classification of data for each subject area. Subject areas are classified as private, proprietary, or both based on the following definitions:

- **Private.** The subject area requires security to protect the privacy of individual participants.
- **Proprietary.** The subject area requires security to protect business sensitive data.
- **Private and Proprietary.** The subject area requires security to protect the privacy of individual participant information and to protect business sensitive data.

Information View Subject Area	Information Security Type
Financial Aid	Private and Proprietary
Transactions & Repayments	Private and Proprietary
FAFSA	Private
Schools	Proprietary
Packages	Private and Proprietary
Participants	Private
Ledgers	Private
Promissory Notes	Private and Proprietary
Organization Information	Proprietary
Customer Service	Proprietary
Organization Review Information	Proprietary
School Enrollment	Private and Proprietary
Management Information	Proprietary
Resources	Proprietary

Table 3-1: Information Subject Area Classification

User Types

Users are classified into types based upon their need for different levels of access to data and include:

- Participants, including students and parents
- Guarantors
- Schools
- Lenders
- State Grant Agencies

Access Rights

Tables 3-2 through 3-6 below present the proposed access rights of different classes of users to the subject areas within Project EASI/ED.

The following are the levels of access that users can have for each type of information:

- **C** – user has the ability to create information
- **R** – user has the ability to read information
- **U** – user has the ability to update information
- **Blank** – user has no access rights

Time Period Definitions

Under certain subject areas, there may be additional columns that represent different periods during which the user may attempt to access the respective information. The users' access rights may change depending upon the period during which they attempt to access the information. For subject areas in which access rights differ across time periods for one or more user groups, the time periods are defined by group as follows:

Schools

- **Allotted.** Time period when a dollar amount for a financial aid program has been allotted
- **Awarded.** Time period once a specific dollar amount has been officially designated for a school, for a particular financial aid program

Free Application for Federal Student Aid Information

- **Pre-completion.** The period when the application is being completed, but has not been completed
- **Completed.** Application has officially been completed (i.e., is error free)

Participant Information

- **Pre-school.** Time period before the student is enrolled in school
- **In-school.** Time period when student is enrolled in school

- **Post-school.** Time period once student is no longer enrolled in school

Financial Aid

- **Award.** When financial aid has been awarded to participant
- **Pre-Disbursement/Disbursement.** Period when funds have been awarded or delivered to participant but repayment is not due
- **Repayment.** Period during which funds are being repaid or are due

Promissory Notes

- **Deferment.** Time period when participant has received financial aid funds, but is not currently in repayment, for one of several reasons (.e.g., in school, military, etc.)
- **Repayment.** Time period when participant must repay financial aid funds to the loan holder

Transactions and Repayment Information

- **Award.** When financial aid has been awarded to participant, but before the actual disbursement of funds
- **Pre-Disbursement/Disbursement.** Period when funds have been awarded or delivered to participant but repayment is not due
- **Repayment.** Period after funds are being repaid or are due

Organization Review Information

- **Appeal.** Time period when a review is under appeal by the respective organization
- **Post-appeal.** Time period when a review is no longer (or never was) under appeal by the organization

SCHOOLS			
School Information	C,R,U		
School Surety Information	C,R,U		
	Overall	Individual Rating	
School Performance Rating	R	C,R,U	
Program Participation Agreement	C,R,U		
School Financial Information	C,R,U		
	Allotted	Awarded	
Award Information	R	R	
FINANCIAL AID PROGRAM INFORMATION			
Financial Aid Program Information	R		
ORGANIZATION INFORMATION			
General Organization Information	R		
	Overall	Individual Rating	
Organization Performance Rating	R	C,R,U	
Accrediting and Licensing Information	R		
Organization Application Information	R		
Low Income Rank Information	R		
FREE APPLICATION FOR FEDERAL STUDENT AID	Pre-completion	Completed	
FAFSA Information	C,R,U	R	
Participant Income	C,R,U	R	
PARTICIPANT INFORMATION	Pre-School	In-school	Repayment
General Information	R,U	R,U	R,U
Benefit Information	R,U	R,U	R,U
Employment Information	R,U	R,U	R,U
Illness Information		R,U	R,U
Skiptrace Information		R,U	R,U
Credit Rating		R	R
Debt	C,R,U	C,R,U	C,R,U
Waiver Information	R,U	R,U	R,U
Income	R,U	R,U	R,U

Table 3-2: User Access Rights: School View

Financial Aid History	R	R	R
Financial Simulation Model			
Social Security Number	R,U	R,U	R,U
Drug Conviction (possibly unavailable in future)	R,U	R,U	R,U
Garnishment and Tax Information			
Bankruptcy	R	R	R
Test Scores (Ability to Benefit test)	R	R	R
PACKAGES			
Package Information	C,R,U		
FINANCIAL AID	Award	Pre-disbursement/Disbursement	Repayment
Basic Financial Award Information	C,R,U	C,R,U	R
Aid Repayment Information		C,R,U	R
Aid Collection Information			R
Aid Participant Information (role, e.g., student, parent)	C,R,U	C,R,U	R
Aid Consolidation Information		R	R
Aid Pre-disbursement Information	C,R,U		R
Aid Status Change Information	C,R,U	C,R,U	R
Aid Discharge Information			R
PROMISSORY NOTES	Award	Pre-disbursement/Disbursement	Repayment
Promissory Note Information	C,R,U	C,R,U	R
TRANSACTIONS AND REPAYMENT INFORMATION	Award	Pre-disbursement/Disbursement	Repayment
Transaction Information		C,R,U	C,R,U
ORGANIZATION REVIEW INFORMATION	Appeal	Post Appeal	
Review (Only non-private information would be available)	R	R	
Deficiency Information	R	R	
Sanction Information	R	R	
SCHOOL ENROLLMENT			
School Enrollment	C,R,U		
LEDGER			
Ledger Information			
MANAGEMENT INFORMATION			
Program Document Information	C,R,U		
RESOURCES			
Resource	C,R,U		

Table 3-2: User Access Rights: School View (continued)

SCHOOLS			
School Information	R		
School Surety Information	R		
	Overall	Individual Rating	
School Performance Rating	R	C,R,U	
Program Participation Agreement	R		
School Financial Information	R		
	Allotted	Awarded	
Award Information	R	R	
FINANCIAL AID PROGRAM INFORMATION			
Financial Aid Program Information	R		
ORGANIZATION INFORMATION			
General Organization Information	R		
	Overall	Individual Rating	
Organization Performance Rating	R	C,R,U	
Accrediting and Licensing Information	R		
Organization Application Information	R		
Low Income Rank Information	R		
FREE APPLICATION FOR FEDERAL STUDENT AID	Pre-completion	Completed	
FAFSA Information	C,R,U	R	
Participant Income	C,R,U	R	
PARTICIPANT INFORMATION	Pre-School	In-School	Post-School
General Information	C,R,U	C,R,U	R,U
Benefit Information	C,R,U	C,R,U	C,R,U
Employment Information	C,R,U	C,R,U	C,R,U
Illness Information	C,R,U	C,R,U	C,R,U
Skiptrace Information	R	R	R
Credit Rating	R	R	R
Debt	R	R	R
Waiver Information	R,U	R,U	R,U

Table 3-3: User Access Rights: Participant View

PARTICIPANT INFORMATION (Continued)	Pre-School	In-School	Post-School
Income	R	R	R
Financial Aid History	R	R	R
Financial Simulation Model	C,R,U	C,R,U	C,R,U
Social Security Number	R	R	R
Drug Conviction (possibly unavailable in future)	R	R	R
Garnishment and Tax Information	R	R	R
Bankruptcy	R	R	R
Test Scores (Ability to Benefit test)	R	R	R
PACKAGES			
Package Information	R,U*	*Possibly C if additional funds needed (.e.g., PLUS loans)	
FINANCIAL AID	Award	Pre-disbursement/Disbursement	Repayment
Basic Financial Award Information	R	R	R
Aid Repayment Information		R	R
Aid Collection Information		R	R
Aid Participant Information (role, e.g., student, parent)	R	R	R
Aid Consolidation Information		C,R, U	C,R,U
Aid Pre-disbursement Information	R		
Aid Status Change Information	R	R	R
Aid Discharge Information			R
PROMISSORY NOTES	Award	Pre-disbursement/Disbursement	Repayment
Promissory Note Information	R	R	R
TRANSACTIONS AND REPAYMENT INFORMATION	Award	Pre-disbursement/Disbursement	Repayment
Transaction Information	R	R	R
ORGANIZATION REVIEW INFORMATION	Appeal	Post Appeal	
Review (Only non-private information would be available)	R (Status only, must contact org.)	R	
Deficiency Information		R	
Sanction Information		R	
SCHOOL ENROLLMENT			
School Enrollment	R		

Table 3-3: User Access Rights: Participant View (continued)

LEDGER	
Ledger Information	
MANAGEMENT INFORMATION	
Program Document Information	
RESOURCES	
Resource	

Table 3-3: User Access Rights: Participant View (continued)

Lenders (and schools servicing Perkins Loans)

SCHOOLS		
School Information	R	
School Surety Information	R	
	Overall	Individual Rating
School Performance Rating	R	C,R,U
Program Participation Agreement	R	
School Financial Information	R	
	Allotted	Awarded
Award Information	R	R
FINANCIAL AID PROGRAM INFORMATION		
Financial Aid Program Information	C,R,U	
ORGANIZATION INFORMATION		
General Organization Information	R,U	
	Overall	Individual Rating
Organization Performance Rating	R	C,R,U
Accrediting and Licensing Information	R	
Organization Application Information	C,R,U	
Low Income Rank Information	R	
FREE APPLICATION FOR FEDERAL STUDENT AID		
FAFSA Information		R
Participant Income		R

Table 3-4: User Access Rights: Lender View

PARTICIPANT INFORMATION	Deferment	Repayment	
General Information	R,U	R,U	
Benefit Information	C,R,U	C,R,U	
Employment Information	C,R,U	C,R,U	
Illness Information	R	R	
Skiptrace Information	R	R	
Credit Rating	C,R,U	C,R,U	
Debt	C,R,U	C,R,U	
Waiver Information	C,R,U	C,R,U	
Income	C,R,U	C,R,U	
Financial Aid History			
Financial Simulation Model			
Social Security Number	R	R	
Drug Conviction (possibly unavailable in future)	R	R	
Garnishment and Tax Information	C,R,U	C,R,U	
Bankruptcy	C,R,U	C,R,U	
Test Scores (Ability to Benefit test)	R	R	
PACKAGES			
Package Information			
FINANCIAL AID	Award	Pre-disbursement/Disbursement	Repayment
Basic Financial Award Information		C,R,U	C,R,U
Aid Repayment Information		C,R,U	C,R,U
Aid Collection Information			C,R,U
Aid Participant Information (role, e.g., student, parent)	C,R,U	C,R,U	C,R,U
Aid Consolidation Information		C,R,U	C,R,U
Aid Pre-disbursement Information	C,R,U		
Aid Status Change Information	C,R,U	C,R,U	C,R,U
Aid Discharge Information			C,R,U

Table 3-4: User Access Rights: Lender View (continued)

PROMISSORY NOTES	Deferment	Repayment	
Promissory Note Information	R	R	
TRANSACTIONS AND REPAYMENT INFORMATION	Award	Pre-disbursement/Disbursement	Repayment
Transaction Information	C,R,U	C,R,U	C,R,U
ORGANIZATION REVIEW INFORMATION	Appeal*	Post Appeal	
Review (Only non-private information would be available)	R	R	
Deficiency Information	R	R	
Sanction Information	R	R	
SCHOOL ENROLLMENT			
School Enrollment	R		
LEDGER			
Ledger Information	R		
MANAGEMENT INFORMATION			
Program Document Information			
RESOURCES			
Resource	C,R,U		

Table 3-4: User Access Rights: Lender View (continued)

SCHOOLS		
School Information	R	
School Surety Information	R	
	Overall	Individual Rating
School Performance Rating	R	C,R,U
Program Participation Agreement	R	
School Financial Information	R	
	Allotted	Awarded
Award Information	R	R
FINANCIAL AID PROGRAM INFORMATION		
Financial Aid Program Information	R	
ORGANIZATION INFORMATION		
General Organization Information	R,U	
	Overall	Individual Rating
Organization Performance Rating	R	C,R,U
Accrediting and Licensing Information	R	
Organization Application Information	R	
Low Income Rank Information	R	
FREE APPLICATION FOR FEDERAL STUDENT AID	Pre-completion	Completed
FAFSA Information		R
Participant Income		R

Table 3-5: User Access Rights: Guarantor View

PARTICIPANT INFORMATION*	Deferment	Repayment	
General Information	R,U	R,U	
Benefit Information	R,U	R,U	
Employment Information	R,U	R,U	
Illness Information	R,U	R,U	
Skiptrace Information	R,U	R,U	
Credit Rating	R,U	R,U	
Debt	R,U	R,U	
Waiver Information	R,U	R,U	
Income	R,U	R,U	
Financial Aid History	R,U	R,U	
Financial Simulation Model	R,U	R,U	
Social Security Number	R,U	R,U	
Drug Conviction (possibly unavailable in future)	R,U	R,U	
Garnishment and Tax Information	R,U	R,U	
Bankruptcy	R,U	R,U	
Test Scores (Ability to Benefit test)	R,U	R,U	
PACKAGES			
Package Information			
FINANCIAL AID	Award	Pre-disbursement/Disbursement	Repayment
Basic Financial Award Information		R,U	R,U
Aid Repayment Information		R,U	R,U
Aid Collection Information			R,U
Aid Participant Information (role, e.g., student, parent)		R,U	R,U
Aid Consolidation Information		R,U	R,U
Aid Pre-disbursement Information		R,U	
Aid Status Change Information		R,U	R,U
Aid Discharge Information		R,U	R,U

*Any info originated by GA should be updateable by GA

Table 3-5: User Access Rights: Guarantor View (continued)

PROMISSORY NOTES	Award	Pre-disbursement/Disbursement	Repayment
Promissory Note Information		R	R
TRANSACTIONS AND REPAYMENT INFORMATION	Award	Pre-disbursement/Disbursement	Repayment
Transaction Information		C,R,U	C,R,U
ORGANIZATION REVIEW INFORMATION	Appeal	Post Appeal	
Review (Only non-private information would be available)	R	R	
Deficiency Information	R	R	
Sanction Information	R	R	
SCHOOL ENROLLMENT			
School Enrollment	R		
LEDGER			
Ledger Information			
MANAGEMENT INFORMATION			
Program Document Information			
RESOURCES			
Resource			

Table 3-5: User Access Rights: Guarantor View (continued)

SCHOOLS		
School Information		
School Surety Information		
	Overall	Individual Rating
School Performance Rating	R	C,R,U
Program Participation Agreement		
School Financial Information		
	Allotted	Awarded
Award Information	R	R
FINANCIAL AID PROGRAM INFORMATION		
Financial Aid Program Information	R	
ORGANIZATION INFORMATION		
General Organization Information		
	Overall	Individual Rating
Organization Performance Rating	R	C,R,U
Accrediting and Licensing Information		
Organization Application Information		
Low Income Rank Information		
FREE APPLICATION FOR FEDERAL STUDENT AID	Pre-completion	Completed
FAFSA Information		R
Participant Income		R

Table 3-6: User Access Rights: State Agency View

PARTICIPANT INFORMATION	Pre-School	In-School	Post-School
General Information	R	R	R
Benefit Information	R	R	R
Employment Information	R	R	R
Illness Information	R	R	R
Skiptrace Information	R	R	R
Credit Rating	R	R	R
Debt	R	R	R
Waiver Information	R	R	R
Income	R	R	R
Financial Aid History	R	R	R
Financial Simulation Model	R	R	R
Social Security Number	R	R	R
Drug Conviction (possibly unavailable in future)	R	R	R
Garnishment and Tax Information	R	R	R
Bankruptcy	R	R	R
Test Scores (Ability to Benefit test)	R	R	R
PACKAGES			
Package Information			
FINANCIAL AID	Award	Pre-disbursement/Disbursement	Repayment
Basic Financial Award Information			
Aid Repayment Information			
Aid Collection Information			
Aid Participant Information (role, e.g., student, parent)			
Aid Consolidation Information			
Aid Pre-disbursement Information			
Aid Status Change Information			
Aid Discharge Information			

Table 3-6: User Access Rights: State Agency View (continued)

PROMISSORY NOTES	Deferment	Repayment	
Promissory Note Information			
TRANSACTIONS AND REPAYMENT INFORMATION	Award	Pre-disbursement/Disbursement	Repayment
Transaction Information			
ORGANIZATION REVIEW INFORMATION	Appeal	Post Appeal	
Review (Only non-private information would be available)		R	
Deficiency Information		R	
Sanction Information		R	
SCHOOL ENROLLMENT			
School Enrollment			
LEDGER			
Ledger Information			
MANAGEMENT INFORMATION			
Program Document Information			
RESOURCES			
Resource			

Table 3-6: User Access Rights: State Agency View (continued)

3.3.4 User Authentication and Authorization Requirements

This subsection will describe the technical requirements for user authentication and authorization. It consists of two parts. Subsection 3.3.4.1 contains requirements for user authentication, including specific requirements for technologies used, and subsection 3.3.4.2 contains requirements for user authorization.

3.3.4.1 Authentication

This subsection describes user authentication requirements. The key concepts and mechanisms for user authentication are described, followed by requirements. Next, issues and strategic findings relevant to Project EASI/ED are discussed. Finally, representative standards and products are presented.

Description: Authentication services must address the need of identifying and authenticating users accessing the system as well as different services communicating with each other in the system. The post-secondary education community, consisting of ED's customers, partners and personnel, is a large group with different backgrounds and characteristics. Authentication mechanisms will have to cater to different needs and risks associated with different users.

Authentication services may be thought of as consisting of the following two components:

- **Identification Mechanism:** mechanism to allow users to identify themselves to the system, e.g., an electronic token
- **Authentication Service:** the service to authenticate users from a list of users and groups

The need for a particular mechanism used will depend on three key factors:

- the type of user, (e.g., participant or school)
- the physical access facility used (e.g., Internet or remote terminal)
- the level of risk associated with the information / subsystem being accessed (e.g., general information about aid program or a financial aid application)

In general, the strength of the identification and authentication mechanism used will depend on the business risk associated with the resource(s) being accessed. The identification mechanism used will depend upon the cost of implementing, maintaining and using the mechanism and the trade-off with the above factors. Different identification mechanisms shall be supported by the system, depending on different combinations of the above three factors.

For example, a lender representative may use digital certificates to authenticate herself while performing financial transactions over the Internet, whereas an ED representative may use a user name and password over a secure terminal in the department.

Authentication mechanisms include:

- **Passwords**

A user authenticates himself or herself by providing a piece of information that only he or she knows. In general, password systems work by requiring the user to enter a user ID and password (or pass phrase or personal identification number). The system compares the password to a previously stored password for that user ID. If there is a match, the user is authenticated and granted access. Passwords are the most common authentication mechanism, and are simple to implement. However the security of the mechanism hinges upon the confidentiality of the password, which can be easily compromised.

- **Security Tokens and Smart Cards**

Security token authentication system combines something the user knows (a PIN) and something the user possesses –(a security token resembling a credit card that continuously generates new passwords that are only valid for a specified duration, according to a formula the company's security server recognizes). The user enters a PIN, and if correct, the card generates the password, which the user enters manually via the PC keyboard. These are far more secure than passwords, but are more costly, difficult to administer and may require special equipment. In addition there are no uniform standards in place.

- **Digital Signatures**

Digital signatures allow the receiver of a digitally signed electronic message to authenticate the sender and verify the integrity of the message. A digital signature is established by creating a message digest of an electronic communication, which is then encrypted with the sender's private key using a public-key algorithm. A recipient who has the sender's public key can verify that the digest was encrypted using the corresponding private key and if the communication has been altered since the digest was generated. Because of the nature of the public-key encryption algorithm, only the public key can decrypt a digest encrypted with the corresponding private key. This process thus establishes that only the holder of the private key could have created the digitally signed message.

- **Biometrics**

Biometric technology involves using a person's unchanging physiological or behavioral characteristics, such as a fingerprint or voice pattern, to verify a person's identity. Common biometric devices include Finger Scanning , Hand Geometry, Dynamic Signature Verification, Voice Verification, Retinal Scan, Iris Scan and Facial Geometry. Biometrics is more secure than most other authentication mechanisms, but is difficult to administer, costly and prone to errors. The lack of widely accepted standards is another hurdle to the adoption of biometrics.

**General
Authentication
Requirements:**

- 6700 There shall be a defined user identification and authentication policy as part of the system-wide security policy covering all the issues related to authentication.
- 6701 Each user of the system shall be uniquely identified, unless the system specifically permits anonymous users in certain situations.
- 6702 The system shall be able to support different mechanisms for identification for each user. (e.g., A student may use an unsecured public internet connection with a electronic token or a secure remote terminal at school with a password)
- User name and password
 - PIN
 - Electronic Token
 - Smart Card
 - Digital Certificate
 - Biometric identification devices
- 6703 The identification mechanism used shall be able to integrate with other security applications.
- 6704 Each user will have appropriate identification codes associated with their identity (e.g., user name, digital certificate or biometric identifier used, as determined by the user identification policy).
- 6705 The identification codes shall be issued securely, possibly physically to the user. This is to prevent compromise of PINs, default passwords, tokens or smart cards.
- 6706 Each user shall be associated with the proper security attributes (e.g., identity, groups, roles, security or integrity levels).
- 6707 The system shall distinguish between different user groups according to the user authentication policy.
- 6708 The system shall have Single Sign-On (SSO) capabilities for all classes of users who need to access more than one system, based on user access rights. This is in keeping with the Project EASI/ED vision of providing a single interface to all users.
- 6709 Interactive Voice Response Units (IVRU) shall ask for appropriate information for identification and authentication, as laid down in the system wide security policy.
- 6710 Information sought by IVRUs to authenticate users shall use information that is used in conjunction with other verification items.
- 6711 The identification code should not be associated with other commonly used numbers or identifiers, such as social security numbers, savings, checking, loan or other financial account numbers, PINs, or the customer's mother's maiden name.
- 6712 The identification code should be unique to the authorized account holder.

- 6713 The identification code should be readily, but securely changed by the authorized account holder.
- 6714 The identification code should be used in association with other customer and account identifiers.
- 6715 The identification and authentication mechanism must be cost effective to use.
- 6716 The identification and authentication mechanisms should be practical and convenient to use for the user.
- 6717 The system shall detect when a specified number of unsuccessful authentication attempts occur.
- 6718 When the defined number of unsuccessful authentication attempts has been met or surpassed, the system shall automatically disable the user account and notify the account holder and system administrator.
- 6719 For all requests for access to services, the requesting host shall be authenticated.
- 6720 There must be specified guidelines to the use of passwords in the Project EASI/ED enterprise-wide security policy.
- 6721 Usernames and passwords shall have a minimum and maximum number of characters.
- 6722 Usernames and passwords shall be composed from a defined set of characters.
- 6723 Default passwords must be changed within a specified time period.
- 6724 A user must be notified of password expiration.
- 6725 Passwords must not be related to the username.
- 6726 Passwords must have a specified frequency of change for all classes of users.
- 6727 Expired or disabled passwords must not be reused for a specified number of generations.
- 6728 There must be specific procedures for password modifications.
- 6729 There must be specific procedures for handling lost passwords.
- 6730 There must be specific procedures for handling password compromise.
- 6731 Passwords must be stored in encrypted form.
- 6732 Passwords must be transmitted in encrypted form.
- 6733 Scripts or messages with embedded passwords must not be used.
- 6734 Access to the password file or database must be restricted to authorized processes.
- 6735 Passwords must be stored as shadow passwords (i.e., the password storage file should not be readable).
- 6736 Login screens must be designed to mask the password characters echo on

User Name and Password / PIN Requirements:

the screen (e.g., for every password character typed by the user an asterisk character “*” should be echoed on the screen).

**Electronic
Token
Requirements:**

- 6737 The electronic token technology chosen must be robust, easy to use and cost effective.
- 6738 The electronic tokens should be usable from all the access points used by the user in question.
- 6739 There must be a specified policy for managing electronic tokens as part of the overall Project EASI/ED enterprise-wide security policy. This will include issuing, validating and disabling electronic tokens.
- 6740 There must be a guaranteed specified maximum time between a report of a lost or stolen electronic token to the time it is disabled.

**Smart Card
Requirements:**

- 6741 Electronic or cards used as one-time password generators must have a specified time cycle of password expiry (e.g., 60 seconds).
- 6742 The passwords generated by one-time password generation electronic tokens or cards must be unique.
- 6743 Smart cards with physical contact reading devices must be rugged and reliable.
- 6744 Smart cards with reading devices must have a specified failure rate.

**Digital
Certificate
Requirements:**

- 6745 An authorized Certificate Authority shall manage all digital certificates.
- 6746 Users need to be able enter the community of key holders, generate keys (or have them generated on their behalf), disseminate public keys, revoke keys (in case, for example, of compromise of the private key), and change keys. In addition, it may be necessary to build in time/date stamping and to archive keys for verification of old signatures.
- 6747 A digital signature as part of the certificate shall use the algorithms specified in the FIPS PUB 186-1 on Digital signatures.

**Biometric
Device
Requirements:**

- 6748 The biometric devices used should be able to support all relevant types of users.
- 6749 The biometric identifier must be unique for each user.
- 6750 The biometric identifier must be a permanent characteristic of the user.
- 6751 The identifier must not cause undue inconvenience to the user.
- 6752 Use of the identifier should conform to acceptable contemporary social standards
- 6753 Specific statistical performance measures for Type I (unauthorized users being authenticated) and Type II (authorized users not being authenticated) errors must be defined for all devices in use.

**World Wide
Web
Requirements:**

- 6754 User authentication over the Web using user names and passwords shall be done using a secure connection based on a protocol such as SSL or SHTTP.
- Please refer to Additional Topics: Web security for additional related security requirements.

**E-mail
Requirements:**

- 6755 Electronic mail services must use an appropriate e-mail encryption technology to authenticate messages.
- 6756 Security sensitive electronic mail messages must use a commonly accepted e-mail security standard such as S/MIME or PGP/MIME.

**Single Sign On
(SSO)
Requirements:**

- 6757 The SSO system should be able to integrate with current ED system security functionality, including IBM RACF security.
- 6758 The SSO product should be able to interface with existing application, database, or network security by way of standard security interfaces. This will ensure that the SSO product will integrate with currently installed security products.
- 6759 The SSO product should provide the ability to enforce security rules enterprise-wide regardless of system platform. This will ensure consistent security over resources on all protected platforms.
- 6760 All changes, modifications, additions, and deletions related to SSO should be logged. This ensures that all security changes are recorded for review at a later time.
- 6761 The SSO system should enable the administrator to be able to trace access to systems regardless of system or platform.
- 6762 The SSO system shall provide for the administration of the product from any of the supported platforms. This enables the administrator to support the product for any platform of his/her choice.
- 6763 All SSO mechanism related changes should be made on-line/real-time. The ability to batch SSO related changes together is also important to enable easy loading or changing of large numbers of security resources or users.
- 6764 The SSO system should synchronize security data across all entities and all platforms. This ensures that all security decisions are made with up-to-date security information.
- 6765 The SSO product should feature a common control language across all serviced platforms so that system administrators do not have to learn and use different commands on different platforms.
- 6766 The SSO product should have the ability to restrict or control access on the basis of a terminal, node, or network address. This ability will enable users to provide access control by physical location.
- 6767 All releases of the SSO product should be backward compatible or release independent. Features of new releases should co-exist with current features and not require a total reinstallation of the product. This ensures that the time and effort previously invested in the prior release of the product is not lost when a new release is installed.
- 6768 The SSO product should support a phased implementation to enable administrators to implement the product on individual platforms without impacting other platforms. This will enable installation on a platform-by-platform basis if desired.
- 6769 The SSO product should include a test facility to enable administrators to

test security changes before placing them into production. This ensures that all security changes are tested fully before being placed into production.

- 6770 The interface of security functionality between distributed systems should be adequately controlled. This includes:
- Controls over the linkage between the local control systems and between the local and central control systems, in relation to data passed between the systems
 - Integrity checks over content of transmitted security data at each location.
 - The identification and authentication (certification) of the various distributed system components to each other.
 - The extension of the controls over the modification of systems software parameters for each of the distributed system components.
 - Synchronization of controls across each of the distributed systems components.
- 6771 Security administration of the system should be done from a single point. This enables an administrator to provide support for the product from any one-platform device.
- 6772 The SSO system should be able to support the creation of spans of control so that administrators can be excluded from or included in certain security control areas within the overall security setup. This enables an administrator to decentralize the administration of security functions based on the groups/nodes/domains/enterprises that the decentralized administrator has control over.

Issues and Strategic Findings:

SFA is currently using an Electronic PIN (ePIN) to provide a unique identifier for students wishing to access SFA systems over the Web. The ePIN is currently being used on NSLDS and FAFSA on the Web, and will soon be used on the Direct Loan Servicing System and the Access America for Students SAM Web site. SFA is trying to use the ePIN as a common authentication identifier for multiple systems. This still means that users have to authenticate themselves separately to each system, even though the identifier is the same. According to the Project EASI vision, one of the goals is to provide a single point of access to EASI/ED. This would mean implementing SSO technology in EASI/ED.

While SFA would like to pursue a digital certificate technology solution to provide secure access for students, this is unlikely to be practical in the near term. The mobility of students, and the cost of providing hardware tokens, will make a digital certificate solution difficult to implement. It is however a mechanism that should be investigated for SFA and institutional users.

Representative Standards:

Authentication Protocols

Kerberos: Kerberos is a network authentication protocol designed to let multiple systems exchange information about a user's identity and access privileges in such

a way that no information that could be used to impersonate a user is ever sent across the network. . It is designed to provide strong authentication for client/server applications by using secret-key cryptography. . It works by assigning a unique key, called a ticket, to each user that logs on to the network. . The ticket is then embedded in messages to identify the sender of the message. This system requires not only that passwords are encrypted, but also that all authentication information is time-stamped so that it cannot be recorded by someone monitoring the network and then retransmitted later. . Kerberos uses secret-key ciphers for authentication and encryption and is favored for remote authentication in client/server environments.

Digital Signature

An ISO standard on Digital Signatures (ISO 14888-3), based on the IEEE P1363 and ANSI X9.F1 and X9.63 is under development.

The National Institute of Standards and Technology (NIST) published the Digital Signature Algorithm (DSA) in the Digital Signature Standard (DSS), which is a part of the U.S. government's Capstone project. DSS was selected by NIST, in cooperation with the NSA, to be the digital authentication standard of the U.S. government. The standard was issued on May 19, 1994. DSA is based on the discrete logarithm problem, and can only be used to provide digital signatures.

The FIPS PUB 186-1 on Digital signatures specifies the algorithms that may be used for hashing and digital signatures.

Representative Products:

Authentication Servers: Computer Associates' (CA) ACF2; Hewlett Packard's (HP) Praesidium Authorization Server; IBM's Resource Access Control Facility (RACF), Distributed Computing Environment (DCE) Security Server, and Global Sign-On; Security Dynamics' ACE/ Server and BoKS; and Sun's Solstice Security Manager.

Single Sign On: CKS's MyNet, Fischer's Watchdog, IBM's Global Sign-On (GSO), and Millennium's FirstStep SSO.

Smart Cards and Tokens: Security Dynamics' SecurID, ActivCard S.A.'s ActivCard, First Access LTD's First Access, Certicom's Sigen.

Biometrics: Hi-Key Technologies' Biometric Access Control System, Miros Inc.'s TrueFace, iNTELiTRAK Technologies, Inc.'s Citadel, Mytec Technologies' Touchstone.

3.3.4.2 Authorization

This subsection will describe the requirements for user authorization. The requirements will be followed by representative products.

Description: Authorization is the process of granting privileges to users of system resources. This is done after they have been authenticated in the system. The authorization mechanisms and policies will enforce the Project EASI/ED user access rights detailed in subsection 3.3.3.

This could be done by restricting access to resources and data in several ways. Most commonly, user authorization is based upon user identities or user groups. The privileges are assigned to a user based on access rights as defined for the individual or the group.

Most database management systems have built-in authorization mechanisms, which use users and user groups to grant or deny privileges. The authorization information is in the form of Access Control Lists (ACLs). In addition, software applications have their own authorization mechanisms, where business rules are used to determine what a user can or cannot do on the system. The ED system wide authorization mechanism has to be able to interface with all of these in all systems.

**General
Authorization
Requirements:**

- 6800 Authorization mechanisms must be able to map the system wide user access rights to mechanisms in individual application software and operating systems.
- 6801 Resources such as data files, programs, application systems and sensitive media must be explicitly defined to the security software.
- 6802 It should be possible to assign access rights for all resources in the system to individual users as well as all users in a group, according to a stated policy.
- 6803 Each user of the system shall have well defined access rights to the system, specifying what resources they have access to and what rights they have.
- 6804 Each user shall belong to at least one user group.
- 6805 User authorization shall be done at two levels based on user groups and user identities.
- 6806 User groups will be given generic access to resources based on Project EASI/ED User Types and Access Rights security requirements. For example, a staff user group from a certain school may have read access to that particular school's student applications.
- 6807 Individual users shall be given authorization rights based on their identities, within the resources that their group has access to. For example, the staff from a certain school may have read and update rights to the student application records they are in charge of.

**System
Resource
Requirements:**

- 6808 Users shall be able to grant certain specified privileges to related parties when appropriate. For example, a student may want to grant privileges to his or her parent.
- 6809 Once authorized, users will have definite access time windows within which they can access applications.
- 6810 There shall be a security intrusion detection and monitoring mechanism for detecting and logging unauthorized access to any part of the system.
- 6811 Security firewalls shall be used to prevent access to systems from unauthorized hosts.
- 6812 There shall be adequate access controls over critical system resources including system libraries, system catalogues and directories, program libraries (source, object, executable), data dictionaries, log files, job control statement libraries.
- 6813 The system should include a test facility to enable administrators to test security changes before placing them into production. This ensures that all security changes are tested fully before being placed into production including security testing of password files, privilege definition tables, encryption algorithms and sensitive application data sets.
- 6814 System security related profiles and other security resources shall only be accessible to authorized security personnel.
- 6815 System security related functionality in the system shall only be accessible to authorized security personnel.
- 6816 There must be adequate controls over available functions which could be used to bypass system security. These include:
- Diagnostic tools, data scopes and standard operator functions available which could be used to read or dump storage areas containing sensitive information such as passwords
 - User interrupts which bypass conventional input/output routines and therefore bypass system security
 - Package software supplier-provided default user IDs

**Representative
Products:**

Representative authorization products include CA's ACF2; Hewlett Packard's Praesidium Authorization Server; IBM's RACF, Distributed Computing Environment Security Server, and Global Sign-On; Security Dynamics' BoKS; and Sun Microsystems' Solstice Security Manager.

3.3.5 User Account Maintenance Requirements

This subsection documents the technical requirements for defining, creating, maintaining and deleting users, resource objects, or the authorized privilege relationships between users and resource objects for Project EASI/ED user accounts maintenance.

Description: User account maintenance is an area of system security that is often taken for granted by organizations. The likelihood of a user account being added to the system multiple times is much greater than a user account ever being deleted. This process is a very simple task if it is done routinely but it can easily become a laborious task that never gets done or done correctly. Organizations sometimes find themselves with user accounts for employees that have left the organization but whose accounts have not been inactivated or revoked. Other times, organizations can find themselves with valid user accounts for employees whose functions have changed but whose system privileges have not been restricted based on their new job functions.

From a business perspective, a lack of control in this area can be damaging if individuals gain access to the system and are able to compromise or corrupt the data. The ability to effectively manage user accounts requires a comprehensive review of general and user-specific requirements that must be reviewed and updated on a regular basis.

- General User Account Maintenance Requirements:**
- 6900 All user accounts shall belong to currently authorized users. Identification data must be kept current by adding new users and deleting former users within a definite time period as specified in the Project EASI/ED enterprise-wide security policy.
 - 6901 Responsibility for maintaining user accounts must rest with a defined group of system administrators.
 - 6902 System user accounts shall only exist for authorized users.
 - 6903 Each user shall have a unique, individual account on the system.
 - 6904 There will be no user accounts for groups, i.e., accounts shall be created for individuals and not groups.
 - 6905 Each user shall have only one account on the system, exceptions would be on a case by case basis.
 - 6906 All user accounts shall have a definite time frame of validity.
 - 6907 The system shall maintain a defined set of unique security attributes belonging to individual users, including but not limited to user name or other identifier.
 - 6908 A user account must be associated to each unique identification mechanism for that user, i.e., user name, digital certificate, electronic token, smart card or biometric identifier.
 - 6909 Each user account must belong to a user type.
 - 6910 Username and group name structure shall be standardized enterprise-wide (e.g., number of characters, composition).

- 6911 Users and user groups must be managed by the system administrator (or equivalent), not by users themselves.
- 6912 Usernames and passwords shall not be distributed in the same communication (e.g., e-mail or fax communication).
- 6913 There must be a defined policy and procedure for disabling or restricting accounts in response to security violations.
- 6914 User accounts shall be disabled or revoked after a specified number of unsuccessful access attempts.
- 6915 User accounts shall be disabled or revoked after a specified period of inactivity. Users will be informed that their account is being disabled if applicable.
- 6916 There must be a specified procedure for creating, suspending, restricting and removing user accounts for each class of user.
- 6917 User rights or permissions access shall be reviewed whenever changes are made to the system or user account.
- 6918 There shall be regularly enforced (e.g., 30 days, 60 days) mandatory user initiated password changes for all system user accounts.
- 6919 User accounts will be restricted from performing multiple concurrent logins using the same user login and password.
- 6920 Audit trails shall exist to log authorized system access and resource usage, to log unauthorized access attempts, and to log maintenance of security profiles or tables.
- 6921 There shall be mechanisms for communicating to the system and automatic revocation of user access when ED, school, or business partner staff leave or are transferred.

Issues and Strategic Findings:

A major concern for SFA is the decentralized administration of accounts for certain groups of users, e.g., school staff. Local administrators may do account maintenance at local sites, but this needs to be synchronized with the enterprise-wide directory of accounts. All users must have individual IDs. The use of group user IDs is prohibited.

3.3.6 Data Transportation and Encryption Security Requirements

This subsection will describe the technical requirements for protecting the confidentiality and integrity of data transmission using encryption technologies.

First, the requirements for data encryption for Project EASI/ED will be laid out. Next, will be subsections on public key encryption, availability and virus protection.

3.3.6.1 Data Encryption

This subsection describes requirements for data encryption algorithms and practices. The requirements are followed by issues and strategic findings related to encryption that are considered important to ED. Finally, some representative standards and products are described.

Description: Data Encryption provides *confidentiality* and *integrity* of information. Confidentiality and integrity need to be protected, both when information is being transmitted as well as when it is stored.

Encryption is the most important underlying technology for every other security mechanism, because of the above two reasons. Encryption is used not only when business data is being protected, but also for enabling authentication and authorization.

Cryptography uses mathematical algorithms and processes to convert intelligible plain text into unintelligible cipher text, and vice versa. Applications of cryptography include:

- Data encryption for confidentiality
- Digital signatures to provide non-repudiation (accountability) and verify data integrity
- Certificates for authenticating people, applications and services, and for access control (authorization)

There are currently two basic types of encryption systems:

- **Private key encryption**, otherwise known as synchronous encryption. In private key systems, a single key is used both for encryption and decryption, so any two communicating parties both have to possess the same key. Since the same key is used by both parties, the key has to be distributed between those parties. Security of the encryption process is therefore dependent on the secure distribution of the keys, which necessitates complex key management processes.
- **Public key encryption**, also known as asynchronous encryption. In public key systems, an asynchronous key pair is used. The keys are mathematically related such that one key can be used for encryption and the other key in the pair used for decryption. So long as one of the keys in a pair is kept secret, the other key can be freely publicized. When a party sends a message to another party, the sender will encrypt

the message using the recipient's public key. Since the message can only be decrypted using the recipient's secret key, only the recipient will be able to decrypt the message, assuming the recipient has kept the secret key secure. In such a system, both public and secret keys are generated locally, i.e., they do not need to be distributed from a central point. Key distribution is therefore not critical to the overall security of the encryption system.

- General Encryption Requirements:**
- 7000 The system shall use encryption algorithms that are industry and government standards based.
 - 7001 The strength of the algorithm used should depend on the sensitivity of the resource or information being protected.
 - 7002 The algorithms used shall undergo review in case of possible threats - reduction in the security provided through their use, taking into account newly available technology, or mathematical weakness of the encryption algorithm.
 - 7003 All encryption keys must have an agreed-upon limited usage. The same encryption key must be used for only a specified number of times or for a specified period of time.

- Private Key Encryption Requirements:**
- 7004 The system shall use an algorithm with at least the strength of Triple DES, as required in the Draft FIPS PUB 46-3.
 - 7005 The system could potentially use an algorithm based on IDEA or the Advanced Encryption Standard (AES), if finalized by the time.

Issues and Strategic Findings:

The strength of most encryption algorithms rests on the *difficulty* of being able to determine the encryption key. Difficulty means the amount (and therefore, cost) of computing power required as well as the time required. The protection offered by a particular cryptographic algorithm diminishes as time goes by, with an increase in the power of computing commonly available and because of the cost of computing power going down. Therefore what is considered secure today, may not be so a few years from now.

The Data Encryption Standard (DES), hitherto the most widely used private key algorithm, is no longer secure. It is feasible to discover a secret DES key within hours, by using desktop computing power. Therefore most organizations do not use DES. According to the draft FIPS PUB 46-3:

- "Single DES will be permitted for legacy systems only. New procurements to support legacy systems should, where, feasible, use Triple DES products running in the single DES configuration."
- "Government organizations with legacy DES systems are encouraged to transition to Triple DES based on a prudent strategy that matches the strength of the protective measures against the associated risk."

Representative Standards: Private Key Algorithms:

- **DES:** DES, which officially became a U.S. government standard in 1977, is the leading single-key algorithm, with the standard specifying a 56-bit key. However, many experts consider longer key lengths of at

least 90 bits necessary for the future. U.S. military-strength encryption requires key lengths of 1,024 bits or more.

- **Triple-DES:** Encrypts information three times using two different 56-bit keys (the "left" key, which encrypts the data, is used twice), thus increasing the effective key sizes of DES so they are computationally more secure and, therefore, more difficult to break. Triple DES has an effective key length of 112 bits.
- **IDEA:** Encrypts information using a 128-bit key and 8 rounds. IDEA is recognized as a fast, Triple-DES- equivalent cipher. IDEA is considered secure, with no algebraic weaknesses that might make it susceptible to being broken. IDEA can be implemented in software or hardware and has similar performance characteristics to DES
- **Public Key Algorithms:** The most commonly used public-key algorithm is RSA (named after the last name initials of its three inventors). RSA is based on the difficulty of factoring large numbers (typically 129 or more bits). Recommended key sizes are 768 bits for personal user; 1,024 bits for business use; and 2,048 bits for extremely valuable keys such as key of a certificate authority. Other public-key techniques include Diffie-Hellman key exchange and the Digital Signature Standard (DSS). Public key algorithms are a component of public key infrastructure, which is discussed in more detail in the next section.

Representative Products: RSA Data Security Inc. (RSADI) licenses the use of the RSA algorithm to vendors. RSA currently is widely accepted and most vendor products support RSA. Cylink, a competitor of RSADI, is the commercial licensing agent for Stanford University, where the Diffie-Hellman and related Hellman-Merkle algorithms were developed. Elliptic Curve Cryptography (ECC), Random Key Stream (RKS), and Raike Public Key (RPK) are other algorithms that are gaining popularity.

3.3.6.2 Public Key Infrastructure

This subsection describes the requirements to be met by a Public Key Infrastructure (PKI).

Description: Public key cryptography requires a public key infrastructure (PKI), essential services for managing digital certificates and encryption keys for people, programs and systems.

There are five core functional components to a PKI:

- The Certificate Authority (CA), an entity which issues certificates. One or more in-house servers, or a trusted third party can provide the CA function.
- The repository for keys, certificates and Certificate Revocation Lists (CRLs) is usually based on a Lightweight Directory Access Protocol (LDAP)-enabled directory service.
- A management function, typically implemented via a management console.
- A key recovery service. Key recovery is an advanced function required to recover data or messages when a key is lost.
- The Registration Authority (RA), an entity dedicated to user registration and accepting requests for certificates. User registration is the process of collecting user information and verifying user identity, which is then used to register a user according to a policy. This is distinct from the process of creating, signing, and issuing a certificate.

Certificate Authorities

One important difference between single-key and public-key cryptographic systems is the way the keys are managed. The critical issue is how to store and validate users' public keys. One solution to this problem has been to have a trusted third party vouch for the authenticity of the public key, either by storing it in a centralized, online database or by distributing it with a certificate. The certificate--basically a copy of the user's public key that has been digitally signed by a trusted third party--binds the identity of the key holder to the public-key value. The organization or body that performs this binding is known as a certificate authority. A certificate authority starts with a root key that is the foundation of all the other certificates it distributes. Individual companies, organizations, and government agencies can act as certificate authorities for their own internal use with help of commercial products and services.

Through digital signatures and encryption, the PKI will provide four basic security services:

- **Authentication:** Ensures that transmissions and messages, and their originators, are authentic, and that a recipient is eligible to receive specific categories of information.
- **Data Integrity:** Ensures that data is unchanged from its source and has

not been accidentally or maliciously altered.

- **Non-repudiation:** Ensures strong and substantial evidence is available to the sender of data that the data has been delivered (with the cooperation of the recipient), and, to the recipient, of the sender's identity, sufficient to prevent either from successfully denying having sent or received the data. This includes the ability of a third party to verify the integrity and origin of the data.
- **Confidentiality:** Ensures that information can be read only by authorized entities.

**Public Key
Infrastructure
Requirements:**

- 7006 The PKI technology must be interoperable and extensible, making sure that ED can take advantage of later marketplace changes and improvements.
- 7007 The technology shall be flexible, adaptable, extensible (able to serve users having divergent environments and interests), expandable, scalable (able to support a much larger user base), and interoperable.
- 7008 PKI development must be able to accommodate all existing and projected ED applications and support interfacing with required external systems.
- 7009 The PKI shall meet Minimum Interoperability Specification for PKI Components (MISPC), that was jointly developed by The National Institute of Standards and Technology (NIST) and The Federal Public Key Infrastructure (FPKI) with leading PKI technology developers.
- 7010 The PKI itself must be secure.
- 7011 The PKI must protect the confidentiality, integrity and availability of the PKI services, for example key generation, key distribution, and key storage.
- 7012 The PKI must provide strong non-repudiation services for actions of certificate services.
- 7013 The PKI must prevent PKI services themselves from repudiating their own actions.
- 7014 The PKI must prevent users and subscribers from repudiating their own actions.
- 7015 The system shall use the services of a trusted certificate authority to manage the distribution of public keys.
- 7016 Each key-holder must be identified uniquely, with the public key itself a strong possibility for that identification.
- 7017 There must be a specified procedure for confirming the identity of a certificate holder (identity proofing), in line with ED and federal government security policies.
- 7018 The identity proofing mechanism must gather proofs of identity that can be linked to legacy databases to verify the existence of the individual user.
- 7019 The identity proofing mechanism must incorporate methods to verify

the identity being "proofed" belongs to the individual requesting the certificate.

- Key Management Requirements:**
- 7020 The identity proofing mechanism must cross-verify the set of data elements as part of the verification process.
 - 7021 The identity proofing mechanism must be in compliance with the Privacy Act.
 - 7022 A certificate holder must be able to delegate permissions he acquires through the certificate to other key-holders, in order to discourage sharing of keys.
 - 7023 There shall be a specified validity period for each digital certificate.
 - 7024 A universal, networked time service must be available for time stamping.
 - 7025 It must be possible to check the validity of each certificate against a Certificate Revocation List (CRL).
 - 7026 It must be possible to ensure that only key recovery enabled systems shall be usable within a PKI implementation, where this is required.
 - 7027 The PKI shall specify key recovery functionality for use in environments that require such functionality.
 - 7028 There shall be a specific policy for the protection and recovery of keys. The policy shall define how the keys are to be protected and under what conditions and to whom a key will be made available.
 - 7029 The key recovery policy shall comply with federal standards and legislation.
 - 7030 A key recovery facility shall be unconditionally trusted and be liable to uphold the stated policy with redress for loss arising from failures to uphold policy through contractual liability and penalties.
 - 7031 A key recovery center shall be able to verify the legitimacy of a key submitted to it for storage.
 - 7032 A user of a key recovery repository shall be able to verify that it is an authorized repository.
 - 7033 The PKI shall provide for coordination between the management of public and private keys in PKI and in data recovery centers.
 - 7034 The PKI shall support aging, revocation, and repudiation of keys.
 - 7035 The PKI shall support discretionary key fragmentation between key recovery facilities.
 - 7036 The PKI shall support facilities for the distribution of keys to appropriate storage devices and directories.
 - 7037 The PKI shall support ability of a certification authority to revoke certificates for individual keys under the terms of the applicable policy.
 - 7038 The PKI shall support ability of a certification authority to suspend and reactivate certificates for individual keys under the terms of the

applicable policy.

- 7039 The PKI shall support ability of a certification authority to force delivery of revocation, suspension, and reactivation notices.
- 7040 The PKI shall support facilities to enable a user to repudiate his public key under the terms of the applicable policy.
- 7041 The PKI shall support facilities to enable a user to suspend and reactivate his public key under the terms of the applicable policy.
- 7042 The PKI shall support facilities to enable the user and subscriber to retrieve revocation, suspension, and reactivation notices.
- 7043 The PKI shall support facilities to enable the user and subscriber to determine the status (e.g., revoked or suspended) of a specific certificate.
- 7044 The PKI shall support facilities to enable the archive and subsequent retrieval of certificates in support of the retrieval and verification of long term information in accordance with governance policy.
- 7045 The PKI must support implementations that enable warranted law enforcement retrieval, subject to security policy and authorization compliance and approval.
- 7046 The PKI must support implementations that enable warranted corporate agency retrieval, subject to policy and authorization compliance and approval.
- 7047 The PKI must support implementations that enable warranted individual retrieval, subject to policy and authorization compliance and approval.
- 7048 The PKI shall support an electronic vehicle for the delivery of a notarized electronic warrant, to support the automation of key retrieval under due process (this must be able to take advantage of existing legal agreements)
- 7049 For supporting warranted retrieval, a permanent, non-repudiable and independently verifiable record of encryption key retrieval operations must be maintained.
- 7050 The PKI must provide distributed certificate management functionality, driven by Project EASI/ED requirements
- 7051 PKI implementation must support policing and policy enforcement (PKI governance model), including the following:
- Policy creation and maintenance. The policies include those covering key generation, key recovery, key distribution, revocation, suspension, repudiation, archive and warranted retrieval.
 - Ability to register a key and the binding between the key and a user name.
 - Ability to query which encryption keys are bound to a particular user name

- Policies (for services built on PKI access control) must not be required to be based on individual identity.
- Certification of the binding between a public key and a directory name shall be mandatory
- Certification of the binding between additional attributes and a directory name shall be discretionary
- Auditing and support for the monitoring of policy compliance is required

- 7052 The PKI implementation should provide concurrent support for multiple security policies.
- 7053 The PKI implementation should provide support for exchange of digital certificates.
- 7054 The PKI implementation should provide support for continuance of service in the event of transfer of certificate services from one certification authority to another.
- 7055 Certificate authority policy mapping services to establish cross certification between CAs.
- 7056 The PKI implementation should provide support for arbitration to determine acceptability of certificates in the event of multiple conflicting certification paths.
- 7057 Support for separation of the certification authority and repository functions in accordance with the governance policy. Changes to certificate repositories must be transactional (e.g., two-phase commits).

Issues and Strategic Findings:

Interoperability: According to "Access with trust", a report by the Federal PKI steering committee, "In order to maximize the possibilities for uniform access to government electronic services by the public and to support secure applications between and among different government agencies, the Steering Committee will emphasize the need for interoperability among the various agency pilots. Specifically, the Steering Committee has endorsed the Minimum Interoperability Specification for PKI Components (MISPC) that was jointly developed by NIST with leading PKI technology developers. The MISPC allows great flexibility for agencies because it specifies minimum interoperability, and describes the broad range of considerations to achieve that requirement (.e.g., hierarchical and networked architectures, certificate format and certificate validation path protocols). In general, agencies will be urged to follow two guiding principles: *simplicity* and *modularity* of design, so that the systems are extensible, providing the functionality desired by each group of users without unnecessary expense and effort. Since the public key infrastructure is evolving with changes in the market place, Federal system designs that incorporate these principles not only will be easier to build, but also easier to change."

Key Recovery: Use of key recovery facilities implies acceptance of a mandatory policy for the protection and recovery of keys. The policy shall define how the keys are to be protected and under what conditions and to whom a key will be made available. The mandatory aspect of policy arises as the operations of a key recovery facility may be regulated by legislation or procedures required

under commercial contracts for liability management.

ED plans to replace Title IV WAN with a VPN. The VPN is intended to have PKI capabilities for both on-line users and system-to-system communication.

Due to the mobility of the student population, digital signatures, which are tied to a single PC, will not meet the needs of many of ED's customers. In the short term, ED plans to use ePIN's for authentication of students (see subsection 3.3.4.1).

Representative Standards: An ISO standard on Digital Signatures (ISO 14888-3), based on the IEEE P1363 and ANSI X9.F1 and X9.63 is under development.

The National Institute of Standards and Technology (NIST) published the Digital Signature Algorithm (DSA) in the Digital Signature Standard (DSS), which is a part of the U.S. government's Capstone project. DSS was selected by NIST, in cooperation with the NSA, to be the digital authentication standard of the U.S. government. The standard was issued on May 19, 1994. DSA is based on the discrete logarithm problem, and can only be used to provide digital signatures.

Representative Products: PKI products currently are available from a variety of vendors, including Entrust, GTE, Motorola, and VeriSign.

Network Associates' Pretty Good Privacy (PGP) PKI, takes a slightly different approach to digital certificates. Users certify each other's keys, thus building up a "web of trust." In some ways, this approach is the most basic form of a PKI. Each user essentially has with themselves their own root key with full authority over it. With the PGP system, there is no single (centralized) certifier; instead, the certification function is distributed.

3.3.6.3 Availability

This subsection describes the requirements for availability of security related services in ED systems.

Description: Availability of systems is an important consideration for security, especially for Project EASI/ED, where the system will be open to a large number of users through public networks. This makes the systems open to security risks such as "denial-of-service" attacks. Another concern could be availability of critical security resources such as firewalls or authentication servers. A firewall can be a single point of failure - if the firewall goes down, the entire connection to the Internet can be lost for the duration of the failure.

Requirements related to Enterprise Security (subsection 3.3.8), Physical Access Security (3.3.2), and Authentication and Authorization (3.3.4) also impact availability. Additionally, availability requirements are discussed in Section 4.

**General
Availability
Requirements:**

- 7058 The network administration function must synchronize changes to the network structure and security across all network components and nodes to ensure the continued integrity and availability of the network.
- 7059 Critical security resources such as firewalls and authentication servers must have redundant back up devices against failure.
- 7060 There must be specific procedures for recovery from failure for all resources in the network.

3.3.6.4 Virus Protection

This subsection describes the requirements related to protection against virus and hostile applets at ED. Representative products will also be described.

Description: Viruses and hostile applets are significant threats to any system, especially in a distributed computing environment as Project EASI/ED. The vulnerability is increased further because of the different systems being integrated, which is a complex issue. The vulnerability of the entire system is as much as that of the weakest link.

- Virus Protection Requirements:**
- 7061 Anti-Virus solutions must protect not only individual hosts on a network as well as protect networks against hostile applets and network threats.
 - 7062 All newly procured software must be isolated and tested prior to use.
 - 7063 Users must be prohibited from installing unauthorized software on any ED computer.
 - 7064 Software received must be verified against the software suppliers or distributors installation checklist.
 - 7065 Software must be checked for viruses using a proprietary tool.
 - 7066 Executable programs must be write protected and/or encrypted to prevent modification.
 - 7067 Program and data files must be backed-up regularly.
 - 7068 System memory must be purged prior to running sensitive applications.
 - 7069 Procedures and controls must be in place to detect virus infections.
 - 7070 There must be routine comparison of programs to secure authorized versions.
 - 7071 Checksum routines must be used for verification of programs.
 - 7072 There must be routine monitoring of the modification duties of programs.
 - 7073 Proprietary virus detection software must be used and regularly updated with the latest specific virus checks.

Representative Products: CyberMedia Guard Dog, Network Associates WebScanX, EliaShim eSafe, Digitivity, Finjan, Check Point, and Security-7 have products that counter the hostile applets.

Cheyenne Software's InocuLAN/AntiVirus, Network Associates' (formerly McAfee's) WebShield and GroupShield software and Symantec's Norton's Antivirus for Internet E-mail Gateways are two leading products for networked environments.

3.3.7 System Security Auditing Requirements

System security auditing protects the confidentiality and the integrity of data within the system. Conformance to auditing requirements ensures that EASI/ED system administrators and managers can monitor access to the data within the system to enforce system authorization rules.

Description: Auditing is the process of data collection and analysis that allows administrators and others, such as auditors, to verify that the user and authorization rules produce the intended results as defined in the business policy. Individual accountability for attempts to violate the intended policy can be established by monitoring security events. The monitoring process can be implemented as a continuous automatic function, as a periodic check, or as an occasional verification that proper procedures are being followed. The auditing information may be used by security administrators, internal audit personnel, external auditors, government regulatory officials, and in legal proceedings. The auditing and monitoring functions also document the activities of security administrators and auditors to ensure that they do not abuse their authorized capabilities. This subsection describes the Project EASI/ED technical requirements for system audit data collection and analysis.

- | | | |
|---|------|---|
| General System Security Auditing Requirements: | 7100 | The contractor shall make available personnel, facilities, and ADP resources to assist the ED, its agents, and the General Accounting Office (GAO) systems, operations and audit staff in conducting initial, annual, and random inspections/audits. |
| | 7101 | The contractor shall provide routine access to contract facilities, personnel and records by auditors and other review teams. |
| | 7102 | Provision for the temporary or permanent installation of audit software packages shall also be made. |
| | 7103 | Routine access, document retrieval and installation of audit software packages shall be provided without additional task orders or cost. |
| | 7104 | The contractor shall develop, test and implement the auditability features conforming to the requirements discussed below. |
| Audit Trail Records: | 7105 | The Department shall have the right to order an independent audit of the contractor's adherence to ED and government security and audit requirements. If requested to do so, the contractor shall cooperate with ED or with ED's auditors or agents in support of the activity at no additional cost to ED. |
| | 7106 | The system shall provide an audit trail record for every log-on. |
| | 7107 | The system shall provide an audit trail record for every attempt to read, modify, add, create, or delete information. |
| | 7108 | The system shall provide an audit trail record for every attempted or successful database administrator/administration activities. |
| | 7109 | The system shall provide an audit trail record for every logging of authorized system access and resource usage. |
| | 7110 | The system shall provide an audit trail record for every logging of unauthorized access attempts. |

	7111	The system shall provide an audit trail record for every logging of maintenance to security profiles or tables and use of sensitive commands.
	7112	The system shall provide an audit trail record for every logging of system environmental changes.
	7113	The system shall provide an audit trail record for every logging of privileged user activity.
	7114	The system shall provide an audit trail record for every logging and control of access by third-party software engineers from remote sites.
	7115	The system shall provide an audit trail record for every logging of excessive access.
	7116	The system shall provide an audit trail record for every logging of use of sensitive commands.
Recorded Event, Requirements:	7117	For each recorded event, the audit record shall identify date and time of event.
	7118	For each recorded event, the audit record shall identify the user.
	7119	For each recorded event, the audit record shall identify type of event.
	7120	For each recorded event, the audit record shall identify success or failure of the event.
	7121	For each recorded event, the audit record shall identify name of the object being used or deleted.
Auditing Software Functions:	7122	The system shall provide adequate retention of system log files.
	7123	The system shall provide maintenance of recovery logs.
	7124	The system shall limit the availability of functionality that can be used to override logging parameters.
Access Restriction Requirements:	7125	All access must be explicitly authorized.
	7126	All access violations must be formally reviewed and followed-up by appropriate staff.
	7127	Access restrictions may not be bypassed by privileged programs, users, or utilities.
	7128	Back-ups must be securely stored.
Log Administration and Monitoring Requirements:	7129	The system shall support log administration and monitoring activities including production and review of job accounting reports.
	7130	The system shall support log administration and monitoring activities including documented procedures for follow-up of serious security violations.
	7131	The system shall support production and review of security profile reports.
	7132	The system shall support production and review of user activity reports.
	7133	The system shall provide support for regular IS management review of log of activities.

3.3.8 Additional Topics

There are certain security mechanisms and practices which will be key to the security needs of Project EASI/ED. The topics in this subsection will cover these mechanisms in the following areas:

- The **Enterprise Infrastructure** subsection covers security requirements for Networks and Firewalls and Proxies.
- The **Directory Services** subsection covers the important security requirements that an enterprise wide directory must fulfil.
- The **World Wide Web** security subsection covers the particular concerns and requirements related to access to network over the web.
- The **Database Security** subsection presents the important security requirements for database security.
- The **System Integration** subsection highlights the important requirements for integrating different information systems in an enterprise like ED.

3.3.8.1 Enterprise Infrastructure

This subsection describes the security requirements with respect to the enterprise network infrastructure.

Description: Network connectivity to any computer system substantially weakens the security of the systems accessible over the network and can, in certain instances, reduce the effectiveness of access controls implemented to protect resources on the systems. It is prudent to take substantial steps to reinforce the security of networked computers.

The several components in ED's enterprise network infrastructure must interact with each other as an integrated whole to ensure overall security.

In general, in a distributed system environment, there is need to

- control access to the network itself
- control access to the resources and services provided by the network
- be able to verify that the mechanisms used to control that access are providing proper protection

The last requires security monitoring too. ED security monitoring system and administrators should continue to actively interface with the Federal Computer Incident Response Capability (FedCIRC). FedCIRC provides a central focal point for information systems security incident reporting, handling, prevention and recognition. The purpose is to ensure the federal government has critical services available in order to withstand or quickly recover from attacks against its information resources.

Another very key mechanism for ensuring network security is the firewall. Network firewalls enforce systems security policy by controlling the flow of

traffic between two or more networks. Firewalls often are placed between the organization's network and an external network such as the Internet or a partnering organization's network. However, firewalls also are used to segment parts of corporate networks. A firewall system provides both a perimeter defense and a control point for monitoring access to and from specific networks. Firewalls can control access at the network level, the application level, or both.

Firewalls can defend against attacks ranging from unauthorized access, IP address "spoofing" (a technique where hackers disguise their traffic as coming from a trusted address to gain access to the protected network or resources), session hijacking, viruses and rogue applets, and rerouting of traffic. Firewalls can also protect a site against some denial-of-service attacks.

Firewall implementations fall into four major categories:

- **Application-level proxies.** Application-level proxies (also known as **proxy servers**) are programs that reside on a firewall and relay traffic for a specified application or service. Client applications outside the firewall communicate with the proxy servers instead of directly with the protected application servers. Because there is no direct network connectivity between external networks and the protected server, the protected system is secured from network-level attacks.

In addition to enhancing security, proxy servers can also be configured to offer caching of data, thereby allowing client requests to be served by local proxy. Some popular proxy server security and caching solutions that run on firewall devices include:

- **Circuit-level gateways.** Circuit-level gateways are the default case of a proxy-based gateway, used when no application-specific proxy exists. In this case, the gateway still relays data for a given application back and forth between the internal network and the external network, thus creating a virtual circuit across the gateway. However, the gateway does not perform any control functions at the application protocol. Instead, it merely serves to pass traffic transparently for a given application.

A circuit-level gateway typically is used as part of a gateway that mainly performs application-level proxy and essentially bypasses the control functions of the gateway for a particular application that is deemed not to pose a security threat and for which no application-specific proxy exists.

- **Packet-filtering gateways.** A packet-filtering gateway controls traffic at the network (IP) and transport (TCP) levels. Packet-filtering gateways examine the source and destination addresses of data packets, source and destination service ports, packet types, and packet options. Packets received by these filtering gateways are permitted or denied based on a rule-based access control list. Because packet-filtering gateways actually are passing the original data packet, these firewalls often are routers.

- **Stateful inspection.** Stateful inspection represents the latest generation of packet-filtering firewalls. Rather than examining the contents of each packet using an application-specific proxy or merely looking at the packet's source and destination address using a simple packet filter, stateful inspection firewalls also compare each packet to a "state table." This table keeps track of inbound and outbound connections and the conversation's state and discards packets not part of a valid connection in the proper context.

A final consideration for firewalls is that remote access over commercial telephone lines is still the most common form of remote access. Typically the remote computer uses an analog modem to dial an auto answer modem at the corporate location. The system uses extra passwords and dial-back to authenticate the user. The extra passwords help thwart call-forwarding attacks and attacks on sites that use the same line for dial-up and callback.

Network Security Requirements:

- 7200 There must be a security mechanism to protect all vulnerable access points in the enterprise network.
- 7201 There must be no single points of failure among vulnerable resources in the system.
- 7202 There must be a mechanism to enforce strong authentication for users accessing systems remotely. The remote authentication mechanisms include:
 - Dial-back modems
 - One-time passwords
- 7203 A firewall shall protect the entry point for a remote access node.

Firewall and Proxy server Requirements:

- 7204 A firewall must be a part of a consistent overall organizational security architecture and must support the Project EASI/ED enterprise-wide security policy security policy.
- 7205 A firewall must be able to accommodate new services and needs if the Project EASI/ED enterprise-wide security policy changes.
- 7206 A firewall must be able to deny all services except those specifically permitted.
- 7207 The firewall host machine must be protected by allowing only limited access to it.
- 7208 The firewall must be able to support all standard authentication mechanisms.
- 7209 The firewall should contain the ability to concentrate and filter dial-in access.
- 7210 A firewall must be able to restrict access to internal as well as external sites.
- 7211 The firewall should contain mechanisms for logging traffic and suspicious activity.
- 7212 The strength and correctness of the firewall should be verifiable.

- 7213 There must be multiple points of failure for the firewall. (i.e., if one link in the network is compromised, the network must not be open).
- 7214 In case of remote access through dial-up lines, the firewall must use a secure technology like modem call-back.

Representative Products:

Proxy Servers: Trusted Information System's Internet Firewall Toolkit (FWTK), Network Associates' Gauntlet, Axent Technologies' Eagle and Secure Computing's Sidewinder are some of the major application-level proxy firewalls. Microsoft's Proxy Server, Netscape's SuiteSpot Proxy Server, Inktomi's Traffic Server, Deerfield Communication's WinGatePro, Ostis' WinProxy, Network Appliance's Internet Middleware, Novell's Border Services, MultiTech Systems' Multi-Router Proxy Server, Lucent Technologies' Personal Web Assistant, Spyglass's Prism, Bay Network's Instant Internet, and NEC Technologies' PrivateNet.

Circuit-level gateways: One of the more widely used circuit relays is SOCKS. SOCKS (for SOCKetS) is a circuit-level protocol supported by the IETF.

Stateful inspection: Check Point's Firewall-1 was the first firewall to implement stateful multilevel inspection, other commercial and public domain firewall packages have included stateful packet filters as their core engine, such as Cisco's PIX and Cyber-source's IP Filter software.

3.3.8.2 Directory Services

This subsection will describe security requirements pertaining to directory services.

Description: Directory services are used for storing information about resources in an enterprise, in a standardized and consistent manner so that it can be accessed easily. Information needed in an enterprise directory could be:

- Persons and organizations
- Certificates
- E-mail and postal mailing addresses
- Computer host names and IP addresses
- Voice and fax telephone numbers

The purpose of directory services is to facilitate enterprise wide and inter departmental communications by standardizing the protocols used to access information from different systems. In today's world, phone numbers, e-mail addresses, locations, and titles change too quickly for printed materials to adequately track and consistently maintain them. Distributed electronic directories help bring order out of this chaos. Aside from ordinary contact information, another key use of directories is the storage of user and organization security credentials, such as the digital certificates that are widely used in public/private-key cryptography. Such credentials facilitate secure communications between individuals and organizations worldwide. They are also a critical element in widespread, Internet-based electronic commerce.

Traditionally, enterprise applications have each maintained its own directory data, and synchronization products have been required to maintain consistency between multiple data sets. Such application vendors will increasingly support the use of external directory services via Lightweight Directory Access Protocol (LDAP) interfaces, thereby increasing the advantage of an enterprise wide application directory.

Directory services would be an important technology for ED as it would enable ED to keep a track of its large number of resources, customers, partners and information about them. It is especially relevant in the Project EASI/ED security context because of the increased need to control access to information pertaining to a large number of users and to serve as a repository for enterprise wide security related information like certificates, keys, security rules and user access rights. ED also has a need to govern network performance based on business rules (i.e., policy-based networking). Moreover, Project EASI/ED will possibly involve the integration of myriad legacy, custom-built and COTS applications, which will need to share data about users and other system resources. Therefore, Interoperability is very important to ED.

- Directory Services Requirements:**
- 7215 Directory Services shall be based on globally accepted standards, so as to easily integrate with applications from most vendors.
 - 7216 Access to the directory must be secured by strong authentication.
 - 7217 The Directory shall provide a unified interface to the user, regardless of the physical location of the information accessed, and it shall possess the necessary knowledge to locate requested information, regardless of where the information might be on the network.
 - 7218 The Directory must provide a strong authentication service for access.
 - 7219 The Directory Server must be able to support different Authentication mechanisms as detailed in subsection 3.3.3.
 - 7220 There must be Interoperability between two Directory components i.e., they should be able to exchange Directory operation requests, results and errors without error and with a mutual interpretation of the various parameters and their values which appear in the protocol exchanges. This should be true both for products by the same vendor as well as those by different vendors.
 - 7221 The Directory shall integrate with the entire ED security infrastructure.
 - 7222 The Directory should be able to serve as a Digital Certificate Repository and interact with the rest of the department's PKI.

Representative Standards: ITU X.500 is the ITU-developed international standard for a directory service. These X.500 servers then exchange directory information so that each can keep its local directory information current. Within the standards for directory services, X.509 defines the directory authentication framework and describes public-key authentication, digital signature techniques, certificates, certificate revocation lists (CRLs), and management procedures.

An alternative to the use of X.509 is the currently being developed Simple Distributed Security Infrastructure (SDSI) standard, that uses public-key cryptography combined with mechanisms for defining groups and group membership certificates. SDSI emphasizes linked local name spaces rather than hierarchical global name spaces (as with X.509). SDSI's groups provide simple, clear terminology for defining access control lists and security policies.

The Open Group DCE standard CAE specification C705-1988 defines the X.500 based Directory Services for DCE using concepts of global name spaces and cell name space. It also defines the DCE Security and Authentication Services. Another related standard is the Lightweight Directory Access Protocol (LDAP) standard (IETF RFC 1777:1995). LDAP provides access to the X.500 Directory while not incurring the resource requirements of the Directory Access Protocol (DAP).

Representative Products: Chromatix SafePages, MessagingDirect's MD Directory , Novell Directory Services 8.0 (currently under beta testing, has improved security support in the form of a native public-key infrastructure), Microsoft Active Directory

3.3.8.3 Security over the World Wide Web

This subsection covers the important requirements concerning security issues for access to EASI/ED systems over the World Wide Web.

Description: Given the large number and geographical spread of ED's customers and partners, the Internet and specifically, the World Wide Web is going to be one of the most important ways for customers and partners to access ED's systems. Unfortunately, public Web sites leave organizations vulnerable to a variety of security problems. Public Web sites have also been the entry point for intrusions into organization's internal networks for the purpose of accessing confidential information.

There are three key security objectives for public Web sites:

- To maintain the integrity of the information intended to be published.
- To prevent the use of the Web host as a staging area for intrusions into the organization's network that could result in breaches of confidentiality, integrity, or availability of information resources.
- To prevent the use of the Web host as a staging area for intrusions into external sites, which could result in the organization being held liable for damages.

**General
World Wide
Web Security
Requirements:**

- 7223 Sensitive information transmitted over the Web must be encrypted.
- 7224 The Server and Client must both authenticate themselves in case of sensitive information being transmitted.
- 7225 A filter or a firewall shall be used to restrict traffic from the Web server host to the internal network.
- 7226 Source routing shall be turned off at the router so that the Web server host cannot be used to forward packets to hosts in the internal network.
- 7227 Public servers shall be placed on subnets separate from internal networks.
- 7228 Network routers should be configured to restrict traffic from public servers to internal networks.
- 7229 Authoritative (genuine and correct) copies of the contents of Web site information should be kept on a host separate from and more secure than the Web server host.
- 7230 Network servers should be configured to offer only essential services. This is to ensure that other services cannot be used to attack the host and impair or remove desired network services.
- 7231 All Web servers connected to the Internet will have a firewall between the Web server and internal department networks.
- 7232 Any internal Web servers supporting critical applications must be protected by internal firewalls. Sensitive, confidential, and private information should never be stored on an external Web server.

7233 Project EASI/ED web sites shall comply with federal government and ED Web site hosting standards, policies and guidelines.

7234 A link to the ED standard privacy policy statement shall be placed on the initial (“splash”) page of all SFA Websites.

Java Security Requirements:

7235 If possible, firewalls will be configured to block the reception of applets from external sources and block the distribution of applets outside of internal networks unless authentication technology is used to protect it from untrusted sources.

Representative Standards:

Secure HyperText Transport Protocol. Secure HTTP (S-HTTP) extends the basic HTTP protocol to allow both client-to-server and server-to-client encryption. S-HTTP provides secure communications between a browser and a server to enable commercial transactions for Web-based applications.

Secure Sockets Layer. Netscape’s Secure Sockets Layer (SSL) is used to add security to TCP/IP applications and has become a de facto standard for encryption between browsers and servers. In contrast with S-HTTP, which secures application-to-application communications, SSL provides end-to-end security between browsers and servers, always authenticating servers and optionally authenticating clients.

Transport Layer Security Protocol. Transport Layer Security (TLS) is an IETF proposed standard that provides enhanced communications privacy and security features at the network transport layer. It is based on SSL.

Generic Security Service (GSS) Application Program Interface (API). The GSS API by the IETF provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source level portability of applications to different environments.

Secure Electronic Transactions. The Secure Electronic Transaction (SET) is an encryption protocol standard for secure credit card authorization over the Internet, designed to replace the previous de facto standard SSL.

IP Security. The IP Security (IPSec) standard seeks to address the interoperability issues critical for Internet-based Virtual Private Networks (VPNs), such as ED’s GEIS Gateway VPN. IPSec defines how an application should establish an encrypted pipeline, or tunnel, over the Internet and ensure that applications from different vendors inter-operate.

Open Platform for Secure Enterprise Connectivity. The Open Platform for Secure Enterprise Connectivity (OPSEC) standard promotes interoperability. It is designed to integrate and manage all aspects of distributed network security through an extensible management framework using a combination of published APIs, industry-standard protocols, and a high-level scripting language.

Other related standards, described in this Section, such as S/MIME, PEM-MIME, MOSS, PKI, PGP, RSA, X.500, LDAP, EDI, and X.509 are also

applicable in this subsection.

Representative Products: Axent Technologies' Web Defender, Network Associates' Gauntlet Forcefield.

In general, most Web servers have integrated security mechanisms built into them.

3.3.8.4 EDI Security

This subsection will describe security requirements particular to Electronic Data Interchange (EDI) between ED and its partners. Some representative standards will be briefly described in the end.

Description In the use of EDI, many paper documents are eliminated. As a result, original hard-copy evidence of obligation or commitment by the department, its bidders or contractors, or its other data interchange partners, may not be available. Instead, electronic records must be used. EDI messages become electronic records as they are prepared for transmission and when they are received. Specific activities must be undertaken to assure that EDI messages, as electronic records, are authentic, are properly authorized, and are completely and accurately retained with audit trails for purposes of accountability. Additionally, EDI messages, while being communicated or stored as records, must be protected from loss, modification, or unauthorized disclosure.

- General EDI Security Requirements:**
- 7236 EDI security must be based on widely accepted industry standards.
 - 7237 EDI security standards shall comply with X12 or EDI for Administration, Commerce, and Transport (EDIFACT), both of which have been adopted by FIPS PUB 161-1.
 - 7238 All EDI systems that are sensitive must be identified. (As per Computer Security Act 1987).
 - 7239 There must be a specific security plan for sensitive EDI systems.
 - 7240 Security training must be conducted for personnel involved in the development and operation of EDI systems.
 - 7241 As with the rest of the systems, resources should be allocated according to the risk and magnitude of potential harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained or transmitted by the EDI system.
 - 7242 There must be a specified procedure for message repudiation.
 - 7243 Written agreements with interchange partners shall establish the specific security and authentication mechanisms to be used, and the legal acceptability, to the recipient, of the originator's electronic messages.
 - 7244 Message Integrity shall be ensured for all interchange of data.
 - 7245 Mechanisms to ensure confidentiality of EDI messages shall be employed. EDI messages, even if unclassified, may contain personal data, trade-secret data, sensitive financial data, or other data whose dissemination must be restricted. Technological and/or procedural methods may be employed to achieve the desired limitations on access.
 - 7246 Originator Authentication must be ensured for all EDI messages.
 - 7247 Non-Repudiation of parties involved in an exchange must be ensured for all EDI transactions.

- 7248 Contingency plans should be implemented for all critical EDI infrastructure in case of system failure or degradation.
- 7249 Complete records of EDI interchanges should be maintained.
- 7250 Unauthorized modifications or alterations to records shall be prevented.
- 7251 Modifications or alterations shall be automatically recorded in an electronic audit trail, including precise dates and times.
- 7252 An electronic copy of each transmitted EDI message, together with the proof of approval, should be retained for audit purposes as the audit trail.
- 7253 In case a Value Added Network (VAN) is used, the security procedures and audit trails provided by the VAN should be among the considerations used for VAN selection.

Representative Standards:

The ANSI X12 EDI standards body started formally addressing security in the late 1980's and early 1990's. The EDI community recognizes that security is an extremely important aspect and has motivated it to define a common X12 security approach to apply universally to all X12 transaction sets. The X12 suite offers two basic security services to protect ANSI X12 electronic transactions against the risk encountered when using the Internet for business. These consist of an electronic digital signature and data encryption

Within the set of X12 standards, two security standards are provided: the X12.58 Security Structures Standard, and the X12.815 Cryptographic Service Message (CSM) Standard. X12.58 establishes the basic structures for inserting security services on an X12 interchange. X12.815 establishes a new transaction set whose main purpose is to provide security management functions to support the encryption and data integrity services of X12.58. Web-based EDI uses several of the current Internet standards such as SSL encryption and static passwords, but they tend to be partial solutions that are not unified in a single body of security standards. The current EDI X12 security standards have the potential to be extended to a Web-based EDI platform. A significant challenge for the near future will be to find ways to merge the current and emerging EDI security technologies to offer seamless EDI security.

3.3.8.5 Database Security

This subsection describes database security requirements for Project EASI/ED.

Description Database security involves not only the access controls over the Database Management System (DBMS) and its functions, but also the implementation of data access restrictions within the DBMS system through the use, for example, of features such as field level security.

Database security is crucial because it is the actual mechanism used to protect business data in a system. It integrates with the overall Project EASI/ED system wide security infrastructure and mechanisms for the information system as a whole.

Database security is also one tool that is utilized to implement the User Access Rights discussed in subsection 3.3.3.

For example, in the current NSLDS environment, the RACF integrates with DB2 security, which enforces the database level authorization rights.

Most DBMSs provide security on their own, or with the aid of third party tools. Some provide enhanced levels of security depending on a client's needs, through add-ons and third party software. There are also specialized database security products available.

**General
Database
Security
Requirements:**

- 7254 The Database security environment must be able to integrate with the enterprise wide security environment
- 7255 The Database security environment must be able to integrate with the Application security environments of all the applications that use it.
- 7256 Controls over DBMS resources should be adequately documented and implemented.
- 7257 The DBMS must have user groups set up corresponding to the user classes defined for the system.
- 7258 User views of data corresponding to each user group must be implemented, .e.g., through a data dictionary
- 7259 There must be access controls within the DBMS to protect the data dictionary security profiles.
- 7260 There must be appropriate access controls over the archive and back-up copies of both the DBMS data and the DBMS configuration parameters.
- 7261 There must be screening procedures that ensure consistent security rules are applied to all DBMS and data dictionary data items regardless of the access path taken by a user.
- 7262 There must be appropriate access controls over DBMS internal user and resource profiles.

- 7263 There must be appropriate controls over access to and definition of data held within the DBMS, including:
- Schema definitions for physical database(s) used in hierarchical and network DBMS architecture
 - Sub-schema definitions for logical views of data held within the DBMS
 - Table definitions and the assignment of table authorities or views for relational databases
 - Binding authorities (relational architectures). (Binding is the process of compiling Data Manipulation Language (DML) statements into programs which access relational databases.)
- 7264 There must be adequate controls to monitor and maintain the integrity of the DBMS, including:
- The use of referential integrity functions where these are available
 - Application design to prevent illogical deletion of database records
 - Checkpointing to aid forward recovery
 - Controls within the DBMS or application level code prevents mutual lockout of database records ("the deadly embrace")
 - Pointer creeping and index verification monitoring to verify data relationships
 - Database synchronization across distributed or linked database components.

Representative Products:

Most database servers have security built into them. This includes authentication, authorization and administration.

Vaultbase VaultSecurity, Braintree's SQL<>SECURE are some specialized database security products.

3.3.8.6 System Integration Security

This section describes the requirements with respect to integrating security functions from various systems within Project EASI/ED into a common security service.

Description: EASI/ED is anticipated to comprise multiple application systems that may be COTS, custom developed, or implemented as an outsourced service. A major consideration will be the integration of security functions from these diverse systems, with different operating systems, application software and hardware. During the development of EASI/ED, attention must be paid to the requirement for the eventual integration of these application systems into a single secure operating environment.

- System Integration Security Requirements:**
- 7265 Security functionality from COTS systems must integrate with the Project EASI/ED system-wide security.
 - 7266 Security functionality from custom software systems must integrate with the Project EASI/ED system-wide security.
 - 7267 It must be possible to administer the security for individual COTS systems through a common security administration interface so that individual systems do not have to be separately administered, exposing them to the risk of inconsistency.
 - 7268 It must be possible to administer the security for individual custom software systems through a common security administration interface, so that individual systems do not have to be separately administered, exposing them to the risk of inconsistency.

3.4 Security Awareness

Introduction

Although an increasing number of organizations are implementing information security measures, there remains an undue emphasis on the technical nature of the problems. Security of information systems, as with security in any other field, relates to people - their abilities, weaknesses, and needs. If a corporate security policy is properly promulgated, personnel will be aware of the part to be played by the individual and will work to fulfill their role in ensuring security of information systems. First, there must be a security policy; and, second, it must be promoted.

The need to raise security awareness across a wide range of personnel will require flexible and comprehensive education programs understandable by all. Admittedly, such programs can represent a weighty and continuing overhead, especially for larger organizations. What has been demonstrated by organizations committed to such programs, however, is that raising awareness and educating a wide audience in the basics of computer security will achieve a far more profound, enduring, and cost-effective improvement in information security than any purely technical solution could ever hope to achieve.

The Importance of Security Awareness

It is all too easy for managers and workers alike to ignore the warnings and bury their heads in the sand. "It will not happen here" is still too common an attitude.

Perhaps this is caused to some degree by the computer security industry itself, which has tended to concentrate on the exotic threats and technical solutions, to the exclusion of the more obvious dangers and the mundane ways of improving security standards. Unfortunately, the evidence is now clear that the greatest threat lies not from the sophisticated attack but from the low-tech insider crime and operator error made possible by poor procedures, a lack of work discipline and, most importantly, a lack of awareness of either the risks or the basic countermeasures.

Almost every incident is caused, not by some massive mistake, but by a series of trivial occurrences that combine to form a chain. Break any link in that chain and the incident is prevented. The staff will break that chain, but only if they are alert to the dangers and committed to conscientious operations.

It is probable, therefore, that security and safety standards will improve dramatically if staff awareness can be raised.

Computer security is not simply a technical matter. There is a highly technical element but not all of the answers lie with the equipment. Computer security is just as much a management problem and, as ever, people are the greatest issue. The technical solution has become increasingly difficult, expensive and cumbersome to either achieve or enforce. Involving staff at all levels and encouraging them to discharge their personal responsibilities towards computer and network security is increasingly being recognized as the area of greatest importance and reward.

Key Issues

The need to alert a wide range of personnel about computer security, to greatly differing depths, requires a flexible and comprehensive awareness program, understandable by all, which addresses the following key issues:

- **Make people want to be secure.** Lasting and effective security will only be maintained once staff members are properly motivated towards such a regime. It is this motivation which is the critical factor in any security education program.
- **Display high-level support.** Security will always fail unless it has total commitment and support from the highest levels. Such support must not be silent; it must be visible to staff. Senior management must also be seen to be following the rules themselves or the rules will be debased.
- **Teach people what to do.** Unless staff members know what to do and how to do it, they cannot be expected to perform to the required standards.
- **Encourage people to be alert.** For every security manager or systems supervisor, there may be dozens or even hundreds of other staff. By galvanizing them through an awareness campaign, this whole work force, rather than just a few of its members, can be employed to police and care for the systems and networks. It is important that the organization's culture both enables and encourages staff to report disgruntled or dishonest colleagues, to challenge strangers and to highlight potential or actual security loopholes and weaknesses;
- **Point out the risks.** The starting point for any computer security effort must be an understanding of the risks to the organization and its IS systems. Unless staff members are aware of the dangers they face, they cannot be expected to take appropriate precautions.
- **Prevent.** Prevention must always be preferable to cure. Awareness campaigns must teach avoidance of security incidents in the first place - although, of course, there must also be instruction about follow-up actions, should the worst ever happen.
- **Be comprehensive.** Awareness programs need to address all aspects of security, by considering the complete triad of confidentiality, integrity and availability.
- **Be simple.** Computer security, for most users of most systems, need not be expensive, complicated or overly technical. Many of the countermeasures are straightforward, involving proper organization and the strict enforcement of codes of good practice.
- **Address the widest possible audience.** The more staff at all levels who can be included in awareness campaigns, the greater the proportion of the work force pulling in favor of the security effort. Of this range though, it is most important to win the support of senior management, for without their total commitment there is little chance of any security effort succeeding.
- **Allocate responsibilities.** Unless a security task is specifically allocated to someone, then it simply will not be done. It is essential that everyone is made aware of their individual responsibilities towards security, so that they may place themselves in the overall picture and identify their parts to play.

- **Be positive and persistent.** The awareness campaign must state clearly what it expects of everyone and then it must repeat its message. The more important that message, then the more often it should be repeated and, wherever possible, repeated in a different way each time. The effort should never be relaxed.
- **Be current, relevant and up-to-date.** Keep the awareness campaign fully up-to-date and relevant. Make sure any changes to company policy, especially where they affect computer security practices and procedures, are incorporated into the campaign and brought to the attention of staff. New systems may require extra or different protection and staff must be told of this.
- **Never assume.** Do not assume that any individuals have security knowledge. Tell them.
- **Be two-way.** There must be a proactive element, since staff are bound to have great contributions to make to the security issues. Potential or actual security weaknesses can best be identified by those staff members dealing with the systems every day. Furthermore, a listening attitude by management, especially when things actually happen as a result of suggestions from the floor, should further encourage a positive attitude towards safety and security.
- **Be targeted.** Direct specific awareness issues at specific audiences and in specific ways. The needs of senior management, for example, will differ to those of input clerks and a course designed for all will end up as a success for none. This does not exclude the need for an awareness framework; indeed, it makes the need for that framework even greater.
- **Be entertaining and amusing.** Security will never be the most riveting of topics but it is important that staff are made aware of the issues. Therefore, a lively, entertaining and amusing campaign may stand a better chance of being remembered.
- **Be measurable.** There must be built into any campaign a method for monitoring and testing its effectiveness.

Motivating Staff

Above all else, any security awareness campaign must make people want to be secure. It may be necessary to provide incentives for staff to follow the rules. There must be rewards - real or abstract - reinforcing good behavior and there must be penalties for those who fail their security responsibilities.

A Framework for Awareness Campaigns

This third subsection describes a suggested framework, addressing the issues of who, how and what should be taught.

Who Should Be Taught?

As information systems move away from the mainframe towards the distributed office resource, each person in the organization, from managing director to cleaner, must be made aware of and trained to comply with their individual responsibility towards computer security:

- The **Systems Manager** is the key person for any computer system, with responsibility for all aspects of that system's functioning, including its security. The systems manager will be required to:
 - formulate an appropriate security policy for the system, in line with any higher corporate policies, beginning at the earliest stage of any system design or procurement process;
 - prepare, maintain and enforce clear security operating procedures so that staff adhere to the policy;
 - arrange independent testing of the system's security and respond to subsequent observations and recommendations;
 - report security breaches and incidents to more senior management together with any changes or developments which might affect in any way the security of the system. Any inability to comply with security policies, for whatever reasons, must also be reported; and
 - maintain a suitable business contingency plan and ensure that it is properly tested at regular intervals.

- **Systems Security Officer.** The Systems Manager will not be able to give security the attention it deserves. The daily administration of security should be delegated to a Systems Security Officer who should:
 - maintain all appropriate logs and records and submit them for regular inspection;
 - restrict access, physical and logical, to authorized systems users only;
 - supervise all visitors, including maintenance engineers and other contract staff;
 - control passwords and identification tokens;
 - administer computer documents, ensuring they are properly marked, stored, used and (eventually) destroyed,
 - at regular intervals, inspect off-site data storage facilities and any remote terminals;
 - investigate security breaches and incidents, reporting to the Systems Manager as appropriate; and
 - be available to provide security advice and education to all systems users.

- **System Users** must:
 - be fully conversant with, and follow, the rules and regulations governing the daily use of the computer system. This is a "numbers game"; it is far better to have everyone following the simple rules than a few following the complicated ones;
 - properly classify all data. Users originate most of the information in a computer system. They are best qualified to judge its value; defenses may then be concentrated on the most valuable or most sensitive information or processes;
 - be alert to the actions of others. Challenge strangers, ensure that colleagues follow the rules and report any suspicions to supervisors; and
 - attend security education programs as required.

- **System Development/Maintenance Staff.** Those specialist staff responsible for the development and maintenance of the system, its software and its data, have an especially privileged position. Their skills allow them extraordinary power over the well-being and security of the system and their mistakes, carelessness or dishonesty can have an inordinate effect. It is particularly important that such staff members are aware of their role in maintaining the safety and security of the system. They should be chosen for their security reliability and positive attitude, they must be more closely supervised than staff members with less influence and they must be constantly reminded of the importance of security rules and procedures.
- **Heads of Departments.** Supervisors and managers with responsibility for computer systems must exercise proper control and supervision over the security of those systems. They must, therefore, be aware of this responsibility. This is especially relevant to the highest levels of management within the organization.
- **Corporate Security Manager.** At the highest level, the Corporate Security Manager will be responsible for the security of all computer systems within the organization and should:
 - perform thorough risk assessments to determine the threats against the computing assets and an appropriate measure of security,
 - develop the corporate computer security policy in line with the general and security-specific policies also in force and as appropriate to the identified risk,
 - monitor the development and procurement of new systems to ensure that consistent security is built into them at the earliest stages of the project life cycle, and
 - supervise the work of all departments to ensure that the computer security policy is being followed and enforced;
- **Network Security Managers.** Responsibility for a network's security is notoriously difficult to assign and is easily assumed to be someone else's job. Each network must, therefore, have a named Network Security Manager and each Systems Security Officer on that network should report through to the Network Security Manager on the security of each node; and
- **Auditors.** The internal audit department has responsibility for checking all aspects of an organization's operations and administration. This department, must be conversant with computer security, as it must be conversant with any other discipline and be included within the awareness program.

How Should Concepts Be Taught?

Each of the groups described above will require different levels and types of computer security awareness and training. In addition there will be a variety of computer systems, from stand alone PC to corporate mainframe to networks, each in their turn needing a differing emphasis of security. It is important, therefore, to target each group on each system with an appropriate awareness-technique covering the appropriate material. The differing needs mean that no single method, course, presentation or medium will satisfy everyone:

- **Specialist Computer Security Training.** Anyone specifically tasked with the enforcement of computer security within an organization, at systems department or corporate level, should receive detailed training, given in a number of stages:
 - for Systems Security Officers, to allow them to advise systems staff on the security of their system, monitoring security procedures and providing a first level of help and advice on site, and
 - after successful completion of this first stage of specialist training and perhaps after a period of on-the-job training as a Systems Security Officer, the more able and suited could then return for further training for appointment to departmental or corporate security manager posts.

Clearly, specialist computer security training represents a considerable investment in time, staff and money and may only be appropriate for larger organizations.

- **Security Awareness for Systems Managers.** Systems managers may need a diluted version of the specialist training. They may not need to replicate the detailed work of their security managers, but they need an appreciation of the risks to their systems, the basic countermeasures that should be applied on a daily basis, and the sources of help and advice to which they and their security managers can turn.
- **External Training Courses.** For the smaller organizations without their own training departments and even for the larger organizations for certain training needs, it is often simpler to send students to external training courses.
- **Conferences and Publications.** Conferences are another source of external training, with the added advantage that much of which is discussed at such events is new and as current as it is possible to be. There are a number of journals and periodicals covering the computer security issue and these, too, are a source of much valuable and up-to-date information and comment.
- **Briefings for Senior Management.** On appointment to any senior position, executives should be introduced (possibly for the first time) to computer security. Senior management should be made aware of the importance of their support to the success of the security effort. They should also be convinced of the sense of making as many personnel as possible (including themselves) aware of the risks to the computing function, the possible effects on the welfare of the organization should those risks materialize, and the ways in which adherence to codes of good practice will reduce those risks significantly and cost-effectively.
- **Arrival Briefings.** The opportunity should not be lost during any employment inductions to draw the attention of new staff to the security rules in force, pointing out the penalties for noncompliance. All staff should sign a form indicating that they have read and understood the regulations. Include security requirements in standard job descriptions and contracts of employment. Insist on non-disclosure agreements for those leaving the employ of the organization.
- **Special Interest Training For All Staff.** Management, security staff and systems users should be encouraged to study together and in more detail, any computer security issue which affects or interests them. Special interest seminars might be an appropriate method, it might also be of benefit to link with other organizations, perhaps in the same line of business, since each might have much to both offer and learn.

General Awareness Techniques

General awareness techniques used in many other areas, e.g., health and safety at work, quality assurance and fire safety can also be brought to bear on security awareness. Such general advertising of codes of good security and safety practices should continue at all times and in whatever ways can be devised. Some techniques include:

- Posters. These should be eye-catching, interesting, simple and limited to a small message. They must be rotated regularly to avoid them being overlooked and they should be placed in every possible position to catch attention.
- Newsletters and staff bulletins including security articles and case histories.
- Videos and slide shows with pre-prepared scripts to draw out the main points in discussion. Although expensive to produce in the first instance, they can subsequently be used widely by local security managers, to reduce the cost per head and to provide a consistent message throughout the organization.
- Prizes and awards. Prizes and awards for good security efforts or ideas will reinforce the positive attitude of the organization towards security. To be of greatest value they must be used sparingly but need not necessarily be of great worth. It is more important that the award is made publicly, so that the individual gains both esteem and recognition.
- Competitions are also useful in motivating staff towards good security. Contests might include such things as "the least number of operator errors this month", or "best security log maintained during the year" as categories. Again, the rewards need not be great; a simple trophy would suffice.

Security training and awareness are not once-a-year matters. They represent continuing overhead and the effort should never be relaxed.

What Should Be Taught?

Computer security must address confidentiality, integrity and availability of data. It must include all of the various defenses in depth from organization, to physical, document, personnel, hardware, software and network security, compromising emanations and contingency planning, through to insurance.

Although there is a wide range of personnel needing differing levels of computer security training and awareness, the essential elements are consistent:

- Computer security is essential to the growth and prosperity of the organization. Without it, if some disaster or breach should happen to the computing function, then the very survival of the business might be threatened;
- Computer security is everybody's responsibility. It cannot be ignored, delegated or postponed;
- Computer security need not be intrusive. It does not always have to be overly technical, expensive or complicated. To most individuals within an organization, it should involve no more than the adherence to a set of common sense and reasonable good practices. It does require a consistent effort, though, by everyone at all times;

- Computer security has the support of the highest levels of management and it is expected that everyone will conform;
- Computer security applies equally to all those within the organization. Nobody is exempt. Everyone, regardless of their role or status, is required to be alert and vigilant to attacks, to potential weaknesses in the defenses and to carelessness or non-compliance amongst other staff members;
- Data is the essential asset. Many confuse this with the need to care for the hardware of the system. Whilst the computer system or network will have a capital value, the data contained within it is far more important than the replaceable equipment; and
- The threats to the organization must be comprehensively assessed in order to devise the correct policy.

Having emphasized that security is everyone's responsibility, it is then necessary to describe computer security tasks as appropriate, so that everyone may place themselves in the overall picture and identify their parts to play:

- Describe in general terms the main elements of computer security;
- Describe the purpose of risk analysis and the organization's chosen methodology;
- Show how to draw together all of the elements into the production of a cost-effective, efficient computer security policy, translated then into workable, understandable and achievable security practices and procedures; and
- Stress the importance of awareness amongst systems staff and instruct Systems Managers on the various techniques to help keep security to the front of everyone's minds.

Testing the Effectiveness of Awareness Programs

Any awareness campaign must have built into it a method for testing its effectiveness. This will inevitably comprise a number of essentially subjective measures, based on the observations of those both administering and receiving.

Objective measures of security are notoriously difficult to calculate accurately. Indeed, the ultimate test of all security is that there should be nothing to report, which itself must always bring into doubt, in senior management's eyes and amongst the work force, the point of it all. Security is an overhead which must be justified continuously and security managers must always be alert to the need to display their efforts as contributing to the overall performance of the business. Therefore, any evidence of the worth of awareness campaigns, even that derived subjectively, is important to the continued support of all concerned:

- Course assessment forms should be included, for students to complete at the end of training. Such questionnaires should request comments on the relevance and effectiveness of each element of the awareness program and ask for suggestions to improve the teaching.
- Surveys and questionnaires amongst staff will reveal both the initial level of security awareness and improvements in that awareness as the program progresses. They might even, if constructed and administered carefully, show how long the effects of particular

awareness modules last. If performed face-to-face, they provide security managers useful opportunities to talk with staff and gather valuable feedback. In turn, this chance for staff to influence the awareness program should enhance their positive attitude towards security.

- The frequency and type of security breaches and incidents should be closely monitored. Ideally, the occurrences will diminish as a result of awareness efforts but they will never cease altogether. Such monitoring should, in particular, look for patterns, such as by department, time of day or value. Findings should be compared with any publicly published figures to try to determine the organization's comparative security performance. It should be noted, though, that as awareness increases, so too will the number of reported incidents and suspicions, even though this does not necessarily reflect a decrease in security.

It is possible to test security. The extreme example of this is the so-called tiger-team testing, where an assault by skilled "hackers" is mounted against the operational environment. On a more mundane level, security managers should try to guess user passwords, visit offices during lunch to see if terminals are logged on but unattended, and in a dozen other ways try to test all aspects of a system's daily security routine. It can be treated as a game at first; the staff will probably respond to the challenge. Only for the most serious offences or when blatant contempt for the rules is discovered, should disciplinary action be brought to bear. Also, it is important to positively reinforce staff when they comply with the rules; this will be more effective than simply punishing those few who do not.

Awareness Issues for the Future

There is no doubt that security awareness remains the poor relation of computer security at the moment. There is still not enough recognition, despite an increasing amount of evidence and a growing number of case histories, that training and motivating staff in the basics of computer security produces an impressive improvement in security standards for relatively little investment. Encouragingly, there are a growing number of initiatives to both improve awareness and to discover and coordinate existing work.