



*FSA Students and Financial Partners Portals*  
Security Plan



Security Plan  
FSA Financial Partners Portal - Release 2

4/9/2003

Author: Matthew Wilson  
Last Modified By: Matthew Wilson  
Last Updated: August 30, 2002 8:45 pm  
Version: 1.0



*FSA Students and Financial Partners Portals  
Security Plan*

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Requirements</b>	<b>3</b>
<b>2.1</b>	<b>Purpose</b>	<b>3</b>
<b>2.2</b>	<b>Formal Requirements</b>	<b>4</b>
2.2.1	Roles & Responsibilities	4
<b>3</b>	<b>Security Organization</b>	<b>4</b>
3.1.1	Information Contact(s)	5
3.1.2	Organization Description	6
3.1.3	Assignment of Security Responsibility	6
<b>3.2</b>	<b>System Operational Status</b>	<b>7</b>
<b>3.3</b>	<b>General Description/Purpose</b>	<b>7</b>
<b>3.4</b>	<b>System Environment</b>	<b>8</b>
<b>3.5</b>	<b>System Interconnection/Information Sharing</b>	<b>9</b>
<b>3.6</b>	<b>Sensitivity of Information Handled</b>	<b>10</b>
3.6.1	Laws, Regulations, and Policies Affecting the System	10
3.6.2	General Description of Sensitivity	11
<b>4</b>	<b>Management Controls</b>	<b>16</b>
<b>4.1</b>	<b>Risk Assessment and Management</b>	<b>16</b>
<b>4.2</b>	<b>Review of Security Controls</b>	<b>16</b>
<b>4.3</b>	<b>Rules of Behavior</b>	<b>17</b>
<b>4.4</b>	<b>Planning for Security in the Life Cycle</b>	<b>17</b>
<b>4.5</b>	<b>Authorize Processing</b>	<b>18</b>



## **1 Introduction**

This document describes the security plan added to the architecture of Task Order 79, Students and Financials Partners Portals. The purpose of the security plan is to provide stronger solutions that will enable the following:

- Infrastructure to build security into new client solutions
- Facilities to allow consolidated and centralized security administration
- Proactive compliance checking of application, system, and network security
- Confidentiality, availability, and integrity of systems with the appropriate level of access
- Appropriate awareness levels of security issues throughout the organization.
- Portals security detailed contact information.

The intended audience for this document includes all FSA personnel operating at the Washington D.C. Office and other facilities owned or operated by FSA, Department of Education. The Financial Partners and Students Portals are federal government maintained websites aimed at having users quickly find specific information and news regarding the financial aid community. Both Portals, while very different in content and target audience, effectively serves the same purpose in gathering and organizing a wide array of information and organizing it into a user-friendly “portal,” a website designed with customizable entry points giving users easy access to the range of information. The security plan aims to provide a high-level overview of security-related information of the system (or portals). While the overview mainly focuses on the system itself (environment, contact information, operations, sensitivity), it also contains additional information on security process (using an example), management controls, and definition of information security.

## **2 Requirements**

The single most important element in ensuring secure information architecture is well-recognized security standards and the presence of a knowledgeable and conscientious System Security Officers (SSO). The System Security Officers are the sole point of contacts (POC) for each of the Portals and are responsible for the security tasks and process of the system. Aside from the SSO, the management personnel for each of the Portals also contain security responsibilities in ensuring that the tasks of the System Security Officer are operating effectively and that a back up is in place for these tasks. Finally, the “end-users,” and members of the Portals team that work with the content of the each Portal, must adhere to the security requirements set forth by the security administrator. This section outlines the minimum-security requirements for both Portals.

### **2.1 Purpose**

Both Portals, as will be explained later, are public sites where a wealth of information is stored and is open to the public. Neither site contains high-level sensitive information requiring strict access. However, both sites do contain information whose delivery, content and accuracy are important to those who access the sites. Therefore, a level of security requirements is absolutely necessary to keep the system intact and both sites operating smoothly. There is an agency-wide “information security group,” addressed in the section as well, which serves as a higher-level FSA security administrator of information for the entire agency.



## **2.2 Formal Requirements**

### **2.2.1 Roles & Responsibilities**

This section lists specific job responsibilities related to IDs and passwords for FSA Portals. It is important to note that as technologies evolve and jobs and personnel change, these standards should be updated to reflect any changes in the Portals environment.

#### **2.2.1.1 Management**

Management will be responsible for the following:

- Ensuring that a primary security administrator is assigned for all computing environments.
- Oversight, compliance, and enforcement.

#### **2.2.1.2 Security Administrator**

The Security Administrator will be responsible for the following:

- Implementing the measures set forth in this standard.
- Drafting, publishing, and updating this standard.

#### **2.2.1.3 End Users**

End Users are responsible for the following:

- Protecting the secrecy of their passwords by adhering to these requirements.
- Identifying and preventing problems such as security exposures, misuse or non-compliance.
- If a problem is recognized, notifying a Security Administrator as soon as possible.

## **3 Security Organization**

The following section contains the organization and contact information for the security administrators for both portals. As explained in the previous section, the security administrators are the primary source for any security-type inquiry and responsibility. It is important to keep in mind that both portals team must be aware of the specific issues that the security POC addresses on a daily basis. While each portals team could potentially create a wide spectrum of security questions and scenarios, this security plan addresses what is in place and does not seek to create security tasks.



### **FSA Portals Organization**

Financial Student Aid  
U.S Department of Education  
Washington, DC 20000

This system is maintained by:

TBD – Working on Operations contracts as of Aug 30, 2002

Washington, DC 20000

#### **3.1.1 Information Contact(s)**

### **Information Contacts**

Students Portal System Owner  
Mary K Muncie  
Students Channel, FSA  
U.S. Department of Education  
UCP3 Room 32E3  
830 1st Street, NE  
Washington, D.C. 20202

Financial Partners Portal System Owner  
Johan Bos-Beijer  
Financial Partners Channel, FSA  
U.S. Department of Education  
UCP3 Room 111I4  
830 1st Street, NE  
Washington, D.C. 20202

The Information Security group is responsible for the overall direction of information security in FSA and acts as a central point of contact for all related issues. Information Security is responsible for ensuring compliance with the direction it sets, both at a policy level and for specific technology design and implementation efforts. Functions of the group include:

- Conduct Risk Assessment
- Security Architecture & Process Design
- Research Security Solutions
- Conduct Product and Technology Evaluations
- Develop and Maintain Policies, Procedures, Standards and Guidelines (PPS&G)



- Manage Compliance
- Manage Incidents
- Increase Security Awareness & Facilitate Change
- Develop Security Strategy & Conduct Risk Analysis
- Manage Privacy

### 3.1.2 Organization Description

The Information Security group will initially consist of one resource who acts as Security Administrator. In addition, the management team and end users comprise the “pyramid structure” of the security organization within both portals.

Role	Name	Functions				
		Policy, Tools, Standards	Awareness, Comm.	Security Admin.	Execute	Audit/Review
Security Administrator	<b>Students:</b> Adam Essex <b>FP:</b> Willie Sutton	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>
Management	<b>Students:</b> Mary Kay Muncie <b>FP:</b> Johan Bos-Beijer	<b>X</b>	<b>X</b>			<b>X</b>
End Users	FP Team Students Team		<b>X</b>			

**Table 1. Security Roles and Functions**

For further information on specific job responsibilities and qualifications refer to *Information Security Organization Roles and Responsibilities*.

### 3.1.3 Assignment of Security Responsibility

An individual must be assigned responsibility in writing to ensure that the application or general support system has adequate security. To be effective, this individual must be knowledgeable of the management, operational, and technical controls used to protect the system.

Adam Essex is the current point of contact for security issues for the Students Portal while Willie Sutton holds the same position for the Financial Partners Portal. Their contact information is listed below.



**Security Point of Contact: Students Portal**

Adam Essex,  
Security Point of Contact  
Students channel, Federal Student Aid  
Department of Education

(202) 377-3515

---

**Security Point of Contact: Financial Partners Portal**

Willie Sutton  
Security Point of Contact  
Financial Partners channel, Federal Student Aid  
Department of Education

(202) 377-3320

### **3.2 System Operational Status**

The following is identified as the current System Operational Status.

- *Operational* — The Financial Partners portal and the Students Portal systems are currently operational.

While both portals are currently operational, both also undergo constant minor modifications, such as updating a particular document or contact information. There are current plans to make more significant modifications as a part of future releases.

### **3.3 General Description/Purpose**

#### Students Portal

The general purpose for the Students Portal is to simplify and consolidate all major available on-line resources available to the student community and offers a personalized customized individual portal. The Students Portal is the gateway between the student community and the Federal Student Aid (FSA) administration and includes all necessary



## *FSA Students and Financial Partners Portals Security Plan*

federal financial aid information for education beyond high school. FSA provides financial help for students enrolled in eligible programs at participating schools to cover school (a four-year or two-year public or private educational institution, a career school or trade school) expenses, including tuition and fees, room and board, books and supplies, and transportation. Most federal aid is need-based.

The users and organizations of the Students Portals are external, and high school and middle school students, college students, parents, and non-traditional students.

The Students Portal provides information on the largest source of student aid in America, FSA (FSA provides nearly 70% of all student aid). This information available in the Portal is intended to help make education beyond high school financially possible. The information provided is designed to assist anybody in college planning. It provides the public with access to and information about the products and services that are needed throughout the financial aid process.

### *Financial Partners Portal*

The Financial Partners (FP) portal was designed in close cooperation with partners in the financial aid community. Federal Student Aid (FSA) Financial Partners works in partnership with Guaranty Agencies, Lenders, Servicers, Trade Associations, Trustees, Schools, and Secondary Markets to ensure access for students to Federal Student Loans particularly the FFEL program. In addition, Financial Partners work with State Grant Agencies on the LEAP/SLEAP grant program.

One of the main services the FP portal offers is the ability to conduct business using one of the various system processes by linking to the Financial Management System (FMS), access the Financial Partners Data Mart, and the National Student Loan Data System (NSLDS). Others

Resources and tools are available which will answer your day-to-day business questions and make access to key personnel easier. The Portal includes a library under Financial Partners Publications, a Financial Partners Community Members resource which will give you access to agency, association, and financial institution information, and a Financial Partners Contact Resources which lists the management staff and regional locations. Users can also learn about projects that FSA is currently working on, have completed, or are planning in the future on the Current Activities page.

### **3.4 System Environment**

- The system is connected to the Internet;
- Software is rapidly implemented;



### **System Environment**

The system is physically housed at FSA's Virtual Data Center (VDC) which is operated by a government contractor. The site is not open to the general public.

A portion of the Students Portal is provided by a subcontractor, Xap Corporation. Xap houses its own web servers and database at its headquarters in Culver City, CA. The site where the servers are housed is not open to the public.

- The primary computing platforms used are Sun Unix servers for the web server and application servers. Refer to the Integrated Technical Infrastructure documentation for more detailed information.
- In addition to the web servers and application servers, the ITA environment includes an Oracle database, Autonomy Server(s) used for search functionality, and an Interwoven server used for content management.
- The Portals make use of the VDC's and Xap's connections to the Internet for http and https traffic.

### **3.5 System Interconnection/Information Sharing**

System interconnection is the direct connection of systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection and information sharing and the increased controls required to mitigate those vulnerabilities. The security plan for the systems often serves as a mechanism to affect this security information exchange and allows management to make informed decisions regarding risk reduction and acceptance.

OMB Circular A-130 requires that written management authorization (often in the form of a Memorandum of Understanding or Agreement,) be obtained prior to connecting with other systems and/or sharing sensitive data/information. The written authorization shall detail the rules of behavior and controls that must be maintained by the interconnecting systems. A description of the rules for interconnecting systems and for protecting shared data must be included with this security plan. See Section 4.3, Rules of Behavior.



### **3.6 Sensitivity of Information Handled**

This section provides a description of the types of information handled by the system and an analysis of the criticality of the information. The sensitivity and criticality of the information stored within, processed by, or transmitted by a system provides a basis for the value of the system and is one of the major factors in **risk management**. The description will provide information to a variety of users, including:

- Analysts/programmers who will use it to help design appropriate security controls;
- Internal and external auditors evaluating system security measures; and
- Managers making decisions about the reasonableness of security countermeasures.

The nature of the information sensitivity and criticality must be described in this section. The description must contain information on applicable laws, regulations, and policies affecting the system and a general description of sensitivity as discussed below.

#### **3.6.1 Laws, Regulations, and Policies Affecting the System**

List any laws, regulations, or policies that establish specific requirements for **confidentiality**, **integrity**, or **availability** of data/information in the system. The Computer Security Act of 1987, OMB Circular A-130, and general agency security requirements need not be listed since they mandate security for all systems. Each organization should decide on the level of laws, regulations, and policies to include in the security plan. Examples might include the Privacy Act or a specific statute or regulation concerning the information processed (e.g., tax or census information). If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) are used for computer matching activities.

See Appendix E for reference to the NIST Computer Security Division's Computer Security Resource Clearinghouse (CSRC) Web site. CSRC contains information on a wide variety of computer security resources, including a list of applicable laws and regulations.



### **Applicable Laws or Regulations Affecting the System**

Privacy Act of 1974 (PL-93-579) \*  
Paperwork Reduction Act of 1980 as amended in 1995 \*  
OMB Circular A-123

\* *Currently under review by ED OGC*

### **3.6.2 General Description of Sensitivity**

Both information and information systems have distinct life cycles. It is important that the degree of sensitivity of information be assessed by considering the requirements for **availability, integrity, and confidentiality** of the information. This process should occur at the beginning of the information system's life cycle and be re-examined during each life cycle stage.

The integration of security considerations early in the life cycle avoids costly retrofitting of safeguards. However, security requirements can be incorporated during any life cycle stage. The purpose of this section is to review the system requirements against the need for availability, integrity, and confidentiality. By performing this analysis, the value of the system can be determined. The value is one of the first major factors in risk management. A system may need protection for one or more of the following reasons:

- *Confidentiality*

The system contains information that requires protection from unauthorized disclosure.

### **Example of Information Requiring Protection — Confidentiality**

Timed dissemination information (e.g., crop report information), personal information (covered by Privacy Act), proprietary business information (e.g., business plans).



- *Integrity*

The system contains information, which must be protected from unauthorized, unanticipated, or unintentional modification.

**Example of Information Requiring Protection — Integrity**

Census information, economic indicators, or financial transaction systems.

- *Availability*

The system contains information or provides services, which must be available on a timely basis to meet mission requirements or to avoid substantial losses.

**Example of Information Requiring Protection — Availability**

Systems critical to safety, life support, and hurricane forecasting.

The Portals sites contain information that is public and available already in other Department of Education websites. The confidentiality level of the content in the Students Portal is very low since the information available in the portal is targeted for a very large cross-section of the general public that is seeking information on financial assistance for education, however, personal account information is confidential, and should be protected. The integrity of the information is medium – high. The information that is presented is of critical importance because it must be accurate and up-to date. While the site is targeted for literally millions of students, the information in the Students Portal must exhibit a high degree of integrity for equal and consistent understanding of important news regarding the financial aid community. The availability level of the students Portal is medium to high. The basis for the Students Portal is to provide information and link all sites regarding the financial aid process for students. While some information contains dates and timeline featuring recommended courses of actions in applying for financial aid, the core of the Portals contains information that will remain fundamental every year.

### **Financial Partners**

The confidentiality of the Financial Partners Portal is low. The main users of the site are members of the financial aid community unlike the Students Portal where the information is more generic and open to the public. The FP Portals website houses specific information regarding loans, interest rates, and special programs that are set up for



community members. Being that it is vital for the FP Portals website to present accurate information such as the latest interest rate figures, the integrity of the site is high. The data must be as recent and up-to date as possible because members rely on this information for their services. The availability of the FP Portals is medium – high. While is it very important for the site to keep updated information, it contains specific information that has to be rapidly displayed, mainly the interest rates on loans.

**Protection Requirement Statement**

Confidentiality is not a concern for the content of this system as it contains information intended for immediate release to the general public. The Students Portal does allow users to create an account on the Portal, and that account information must be protected. It is important to ensure the integrity of the information so that the most accurate information is provided to the public. System availability is also a concern as systems users expect a high degree of availability and reliability.

<b>Confidentiality Considerations: Students Portal</b>	
<b>Evaluation</b>	<b>Comment</b>
<b>Medium</b>	<p>The Students Portal mainly disseminates information on financing costs for college and help on a wide array of topics regarding higher education that is also made openly available to the public. It also contains summaries to links that house information on financing college costs and provides information for applying and repaying college loans. None of the information requires protection against disclosure.</p> <p>User account information, however, requires a certain level of protection.</p>

<b>Confidentiality Considerations: Financials Partners Portal</b>	
<b>Evaluation</b>	<b>Comment</b>
<b>Low</b>	<p>The mission of the Financial Partner Portal is to disseminate information that is made available openly to the public. It also contains summaries to links that house information on financing college costs and provides information for applying and repaying college loans. None of the information requires protection against disclosure.</p>



<b>Example Integrity Considerations</b>	
<b>Evaluation</b>	<b>Comment</b>
<b>High</b>	The application is a financial transaction system. Unauthorized or unintentional modification of this information could result in fraud, under or over payments of obligations, fines, or penalties resulting from late or inadequate payments, and loss of public confidence.
<b>Medium</b>	Assurance of the integrity of the information is required to the extent that destruction of the information would require significant expenditures of time and effort to replace. Although corrupted information would present an inconvenience to the staff, most information, and all vital information, is backed up by either paper documentation or on disk.
<b>Low</b>	The system mainly contains messages and reports. If these messages and reports were modified by unauthorized, unanticipated or unintentional means, employees would detect the modifications; however, these modifications would not be a major concern for the organization.

<b>Integrity Considerations: Students Portal</b>	
<b>Evaluation</b>	<b>Comment</b>
<b>Medium</b>	The information, both content and user account information should be backed up daily, to insure that it could be recreated in a timely fashion if required.

<b>Integrity Considerations: Financials Partners Portal</b>	
<b>Evaluation</b>	<b>Comment</b>
<b>Medium</b>	The information stored in the Financial Partner Portal should be backed up daily, to insure that it could be recreated in a timely fashion if required.

<b>Example Availability Considerations</b>	
<b>Evaluation</b>	<b>Comment</b>
<b>High</b>	The application contains personnel and payroll information concerning employees of the various user groups.



*FSA Students and Financial Partners Portals  
Security Plan*

	Unavailability of the system could result in inability to meet payroll obligations and could cause work stoppage and failure of user organizations to meet critical mission requirements. The system requires 24-hour access.
<b>Medium</b>	Information availability is of moderate concern to the mission. Macintosh and IBM PC availability would be required within the four to five-day range. Information backups maintained at off-site storage would be sufficient to carry on with limited office tasks.
<b>Low</b>	The system serves primarily as a server for e-mail for the seven users of the system. Conference messages are duplicated between Seattle and D.C. servers. Should the system become unavailable, the D.C. users would connect to the Seattle server and continue to work with only the loss of old mail messages.

<b>Availability Considerations: Students Portal</b>	
<b>Evaluation</b>	<b>Comment</b>
<b>Medium to High</b>	The Portal includes links to sites and applications relevant to students. Users would still be able to reach those applications, such as the FAFSA, if the Students Portal were unavailable, however, outages are not received well by the user community.

<b>Availability Considerations: Financials Partners Portal</b>	
<b>Evaluation</b>	<b>Comment</b>
<b>Medium to High</b>	The Portal includes links to sites and applications relevant to Financial Partners. Users would still be able to reach those applications, such as FMS or the Datamart, if the Financial Partners Portal were unavailable, however, outages are not received well by the user community.

## **4 Management Controls**

This section, describes the management control measures that are intended to meet the protection requirements of the major application. Management controls focus on the management of the computer security system and the management of risk for a system. The types of control measures shall be consistent with the need for protection of the major application or general support system. To aid the reader, a brief explanation of the various management controls is provided. For more detail on management controls, see NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*.

### **4.1 Risk Assessment and Management**

OMB Circular A-130 no longer requires the preparation of a formal risk analysis. It does, however, require an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system. The methods used to assess the nature and level of risk to the system should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. BSC Systems, the Independent Validation and Verification (IV&V) contractors for the project, have planned a Risk Assessment. The risk assessment is intended to identify threats, vulnerabilities, and the additional security measures required to mitigate or eliminate the potential that those threats/vulnerabilities could have on the system or its assets.

### **4.2 Review of Security Controls**

OMB Circular A-130 requires that at least every three years an independent review of the security controls for each major application be performed. For general support systems, OMB Circular A-130 requires that the security controls be reviewed by an independent audit or self-review at least every three years.

The review or audit should be independent of the manager responsible for the major application or general support system. Independent audits can be internal or external but should be performed by an individual or organization free from personal and external factors, which could impair their independence or their perceived independence (e.g., they designed the system under review). The objective of these reviews is to provide verification that the controls selected and/or installed provide a level of protection commensurate with the acceptable level of risk for the system. The determination that the level of risk is acceptable must be made relative to the system requirements for confidentiality, integrity, and availability as well as the identified threats.



The security of a system may degrade over time, as the technology changes, the system evolves, or people and procedures change. Periodic reviews provide assurance that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection.

The type and rigor of review or audit should be commensurate with the acceptable level of risk that is established in the rules for the system and the likelihood of learning useful information to improve security. Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest hardware/software “patches”), and penetration testing can assist in the ongoing review of system security measures. These tools, however, are no substitute for a formal management review at least every three years.

### **4.3 Rules of Behavior**

The rules of behavior document was prepared for the first release of the Financial Partners and Students Portals. The security required by the rules is only as stringent as necessary to provide adequate security for the system and the information it contains. The acceptable level of risk should form the basis for determining the rules.

The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules should state the consequences of inconsistent behavior or noncompliance. The rules should be in writing and form the basis for security awareness and training.

Rules of Behavior shall also include appropriate limits on interconnections to other systems and define service provision and restoration priorities. They should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability. Rules should reflect administrative and technical security controls in the system. For example, rules regarding password use should be consistent with technical password features in the system. Such rules would also include limitations on changing information, searching databases, or divulging information. Rules of behavior may be enforced through administrative sanctions specifically related to the system (e.g., loss of system privileges) or through more general sanctions as are imposed for violating other rules of conduct.

### **4.4 Planning for Security in the Life Cycle**

Although a computer security plan can be developed for a system at any point in the life cycle, the recommended approach is to draw up the plan at the beginning of the computer system life cycle. It is recognized that in some cases, the system may at any one time be in several phases of the life cycle. For example, a large human resources system may be



in the operation/maintenance phase, while the older, batch-oriented, input sub-system is being replaced by a new, distributed, interactive user interface. In this case, the life cycle phases for the system are the disposal phase (data and equipment) related to the retirement of the batch-oriented transaction system, the initiation and acquisition phase associated with the replacement interactive input system, and the operations/maintenance phase for the balance of the system.

Release 1 of the portals is currently in the operations and maintenance phase, while release 2 is in the implementation phase at the time of publication for this report.

During the implementation phase of release 2, the system's security features should be configured and enabled, the system should be tested and installed or fielded, and the system authorized for processing. (See Section 4.5, Authorize Processing, for a description of that requirement.) A design review and systems test should be performed prior to placing the system into operation to assure that it meets security specifications. In addition, if new controls are added to the application or the support system, additional acceptance tests of those new controls must be performed. This ensures that new controls meet security specifications and do not conflict with or invalidate existing controls. The results of the design reviews and system tests should be fully documented, updated as new reviews or tests are performed, and maintained in the official organization records.

#### **4.5 Authorize Processing**

The term "authorize processing" is the authorization granted by a management official for a system to process information. (Note: Some agencies refer to this authorization as **accreditation**.) Authorization provides a form of quality control and is required under OMB Circular A-130. It forces managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. By authorizing processing in a system, a manager accepts the risk associated with it.

Both the security official and the authorizing management official have security responsibilities. The security official is closer to the day-to-day operation of the system and will direct, perform, or monitor security tasks. The authorizing official will normally have general responsibility for the organization supported by the system. Authorization is not a decision that should be made by the security staff. Some agencies have established the system approval process as a formal accreditation procedure where the approving authority is termed the Designated Approving/Accreditation Authority (DAA). Formalization of the system authorization process reduces the potential that systems will be placed into a production environment without appropriate management review.

Management authorization must be based on an assessment of management, operational, and technical controls. Since the security plan establishes the system protection requirements and documents the security controls in the system, it should form the basis for the authorization. Authorization is usually supported by a technical evaluation and/or



*FSA Students and Financial Partners Portals*  
Security Plan

security evaluation, risk assessment, contingency plan, and rules of behavior. Note: Some agencies refer to the technical evaluation and/or security evaluation as a certification review. Re-authorization should occur prior to a significant change in the system, but at least every three years. It should be done more often where there is high risk and potential magnitude of harm.

Below are the minimum security controls that must be in place prior to authorizing a system for processing. The level of controls should be consistent with the level of sensitivity the system contains.

- Technical and/or security evaluation complete.
- Risk assessment conducted.
- Rules of behavior established.
- Contingency plan developed and tested.
- Security plan developed, updated, and reviewed.
- System meets all applicable federal laws, regulations, policies, guidelines, and standards.
- In-place and planned security safeguards appear to be adequate and appropriate for the system.
- In-place safeguards are operating as intended.