

***FSA Modernization Program***  
**United States Department of Education**  
**Federal Student Aid**



**Single Sign-On**  
**Preliminary Risk Assessment**

***Task Order #82***  
***Deliverable #82.1.6***

**Final**

**May 17, 2002**

## Document Revision History

| Version No. | Date         | Author        | Revisions Made         |
|-------------|--------------|---------------|------------------------|
| 1.0         | May 17, 2002 | Michael Bruce | Initial draft released |
| 1.1         |              |               | Revised draft released |
| 1.2         |              |               | Final draft released   |
|             |              |               |                        |

## Table of Contents

|  |           |
|--|-----------|
| <b>EXECUTIVE SUMMARY .....</b>                       | <b>4</b>  |
| <b>1 INTRODUCTION .....</b>                          | <b>5</b>  |
| <b>2 PROJECT DESCRIPTION.....</b>                    | <b>6</b>  |
| <b>2.1 Objective.....</b>                            | <b>6</b>  |
| <b>2.2 Scope .....</b>                               | <b>6</b>  |
| <b>2.3 Project Identification.....</b>               | <b>7</b>  |
| <b>2.4 General System Information.....</b>           | <b>7</b>  |
| <b>3 SENSITIVITY AND PRIVACY .....</b>               | <b>9</b>  |
| <b>3.1 Sensitivity/Privacy Determination.....</b>    | <b>9</b>  |
| <b>3.2 Sensitivity Determination.....</b>            | <b>16</b> |
| <b>4 SYSTEM AVAILABILITY .....</b>                   | <b>18</b> |
| <b>5 RECOVERY OBJECTIVE.....</b>                     | <b>20</b> |
| <b>5.1 Identification of Impacts over Time .....</b> | <b>20</b> |
| <b>5.2 Summary of Impacts .....</b>                  | <b>21</b> |
| <b>5.3 Internal and External Dependencies.....</b>   | <b>22</b> |
| <b>6 SECURITY REQUIREMENTS .....</b>                 | <b>23</b> |
| <b>7 ADDITIONAL RISKS .....</b>                      | <b>26</b> |

## EXECUTIVE SUMMARY

The Single Sign-On initiative at FSA is intended to develop and deploy a common and reusable Identification and Authentication (I&A) infrastructure. Additionally the effort intends to develop a common system enrollment process for business applications utilizing this I&A infrastructure.

In order to successfully plan and manage the development of this service, the IPT team has identified the following business, technology, and security that must be addressed and mitigated during the development, deployment, and operations of FSA's single sign-on service:

- **Certification and Accreditation** – Upon IRB approval of Phase III, FSA will need to appoint a system manager and systems security officer for the single sign-on service. These individuals are responsible for ensuring the service meets all FSA requirements for deploying a production business application.
- **General Support and Operations** – Upon deployment into production, the single sign-on service must be operated in a secure manner and in a secure facility. The system configuration must be documented, and trained support staff available to resolve operational issues.
- **Confidentiality/Sensitivity** – Depending upon the final approved detailed design for the single sign-on service, the application may contain information deemed sensitive or privacy protected. This information may be part of the user enrollment data (e.g., name, email address, authentication questions and answers) or part of the access credential data (e.g., SSN, date of birth).
- **Criticality/Availability** – The single sign-on service will require a high-level of availability since it will provide access control and user I&A services to business applications that adopt this service. If the service does become unavailable, there will be no significant short-term (i.e., system is not available for less than 24 hours) impacts to FSA based upon the current systems expected to use the service. However this will not be the case if FSA or ED business applications that affect program eligibility, student eligibility, or the movement of money are impacted.
- **Security Threats** – The business risks caused by potential security threats to the service are Moderate to Low. In all cases, the likelihood of potential threats is Low and the impact of a potential threat is High resulting in, at most, a Moderate business risk to FSA.
- **Additional Risks** – Additional business risks can affect FSA business strategy, the FSA organization, financial or other resources, project management, business operations, data / information, applications, technology infrastructure, security, and privacy. Possible risk, probability/likelihood, impact, and a strategy to manage each of these risks have been identified. There are no items for which a management or risk mitigation strategy is not available.

## 1 INTRODUCTION

This Preliminary Risk Assessment represents an initial identification of business, technical, and operational risk. This document serves as a pre-cursor to addressing the security needs for the implementation of a single sign-on service at Federal Student Aid (FSA). Upon approval of the Phase III business case, this effort will need to initiate FSA's certification and accreditation process that this project must complete in order to satisfy Production Readiness Review (PRR) requirements. This document attempts to classify and identify risks and potential security needs for the Single Sign-On Phase III development and deployment effort.

The Preliminary Risk Assessment is composed of the following sections:

- Project Description and Identification – describes the system and responsible parties.
- Sensitivity – establishes the classification level associated with confidentiality and integrity.
- Criticality – establishes the classification level associated with unavailability.
- Recovery Objective - establishes the maximum allowable downtime for the system.
- Security Requirements – identifies potential threat events and business impacts.
- Additional Risks – identifies additional business and/or technology risks

## 2 PROJECT DESCRIPTION

As part of its commitment to customers and partners, FSA manages risk on a continuous basis. In view of this, FSA recognizes that there is a need to provide system access controls that enhance a user's online experience allowing for a closer relationship to FSA and greater reliance upon FSA services and applications. At the same time access services must adhere to ED/FSA identification and authentication policies, and U.S. Public Law and policy.

Currently, system users may utilize multiple access credentials to logon to FSA systems. This places the unnecessary burden on users of having to remember multiple username/password combinations. Approximately 30,000 School and Financial Partner users access FSA systems on a regular basis as part of regular student financial aid processing and administration. Over 26 million students have on-line access to FSA systems in order to complete FAFSA submissions and conduct other student aid related business.

In addition, as new and reengineered systems are released, additional access credentials and rights may also be created. This could create increasing opportunities for unauthenticated access to FSA systems, undermining the credibility of FSA, and affecting its ability to help put America through school. To reduce the risk inherent in multiple access points, a Single Sign-On service is being developed.

### 2.1 Objective

The intent of this document is to define the high-level business, technology and security risks for the development of a Single Sign-On service for FSA systems. The key objectives of this document are to:

- Identify potential risks that apply to the operation of a Single Sign-On service for FSA system users and administrators.
- Identify potential confidentiality and privacy issues that a Single Sign-On service must address during its development and deployment.

### 2.2 Scope

This document defines the potential risks for a Single Sign-On service for FSA systems. These risks are based on the business and technical requirements, general design, and alternatives analysis completed by an enterprise IPT, and discussions with channel stakeholders. The IPT leveraged guidance from the Single Sign-On advisers throughout the process.

It is anticipated that an FSA Single Sign-On service can provide the following benefits:

- Improved customer access to FSA systems – [Common](#) Identifier and [Common](#) Enrollment
- Support the access needs for FSA's Portals and overall eCommerce strategies
- Strengthened cyber-security – [Trusted](#) Identifier
- Establish a [Reusable](#) Single Sign-On infrastructure for FSA systems
- Provide potential future economic [Savings](#):
  - System enrollment
  - User access management

- o Reduced customer support for login

### 2.3 Project Identification

The following provides general information concerning this initiative:

|                                  |  |
|----------------------------------|--|
| <b>System Name:</b>              | FSA Single Sign-On   |
| <b>Executive Sponsor(s):</b>     | Steve Hawald<br>Kay Jacks  |
| <b>Program Manager:</b>          | Charlie Coleman  |
| <b>Project Manager:</b>          | Neil Sattler   |
| <b>System Owner:</b>             | To Be Determined Upon Phase III Approval   |
| <b>System Security Officer:</b>  | To Be Determined Upon Phase III Approval   |
| <b>Development Site:</b>         | To Be Determined Upon Phase III Approval   |
| <b>Production Site(s):</b>       | Expected to be: FSA Virtual Data Center, operated by CSC Corporation, and located in Meriden, CT.  |
| <b>Platform:</b>                 | To Be Determined. The current ITA standard hardware platforms supported by the VDC are Hewlett-Packard HP-UX (preferred) and Sun Solaris.  |
| <b>Brief System Description:</b> | To provide common and reusable user identification and authentication service for selected new and modernized FSA business applications. This effort will also provide a common enrollment service for these same selected new and modernized FSA business applications. |

### 2.4 General System Information

The following questions provide insight into the nature of the application, and its operating environment.

|    | <b>General System Data</b>   | <b>Yes</b> | <b>No</b> |
|----|--|------------|-----------|
| 1. | Will the system be developed or managed primarily by non-government personnel?<br><br>The system will be developed by an FSA designated contractor, and is expected to be operated at FSA's primary data center – the VDC – managed by an FSA operating partner. | X          |           |
| 2. | Will the system be located in an ED/FSA controlled access area?<br><br>Yes, the VDC.   | X          |           |
| 3. | Is a GOTS/COTS product a significant feature or portion of the information resource?   | X          |           |

|     | <b>General System Data</b>  | <b>Yes</b> | <b>No</b> |
|-----|---|------------|-----------|
|     | resource?<br><br>The IPT recommends a COTS (IBM/Tivoli's Access Manager and Identity Manager product) approach for developing and deploying the single sign-on service.   |            |           |
| 4.  | Does the GOTS/COTS application contain custom programming or scripts?<br><br>Some development of custom scripts and custom code is expected.  | X          |           |
| 5.  | Is the system an externally facing application containing custom programming (html, XML, Java, Javascript, CGI, ActiveX, etc)?<br><br>Some development of custom scripts and custom code is expected.   | X          |           |
| 6.  | Is a database solution used to process and store information?<br><br>The system will use on ODBC database or an LDAPv3 repository for user credential and data storage.   | X          |           |
| 7.  | Does the system have access to or communicate through an untrusted network?<br><br>Yes, users will access the single sign-on service via the public Internet.   | X          |           |
| 8.  | Does the application contain transmit information between a trusted network and a public, un-trusted network or between an FSA demilitarized zone (DMZ) and an untrusted network?<br><br>Users will transmit some information (i.e., user access credentials) over the Internet (un-trusted public network) to the single sign-on service. The single sign-on service will send information back to a user's browser over the Internet. In both cases, the exchange of information will be over an SSL 128-bit encrypted session. The SSL session will be maintained by the single sign-on service. | X          |           |
| 9.  | Will performance issues have a significant impact on the FSA mission?<br><br>Yes, if users are unable to be authenticated by the single sign-on service so that they can utilize FSA business applications that are protected by the Identification & Authentication portion of this service, FSA customers will be unable to conduct business with FSA.  | X          |           |
| 10. | Will system backups be stored at an FSA controlled access area?<br><br>System backups will be performed by FSA's data center operating partner on-site at the data center. The backups will be stored as designated by this operating partner as approved by FSA.   | TBD        |           |
| 11. | Will system backups be stored off-site at an FSA controlled access area?<br><br>System backups will be performed by FSA's data center operating partner on-site at the data center. The backups will be stored as designated by this operating partner as approved by FSA.  | TBD        |           |

### 3 SENSITIVITY AND PRIVACY

#### 3.1 Sensitivity/Privacy Determination

The following identifies potential sensitivities for privacy and confidentiality by the singles sign-on service.

##### Part I: Sensitivity Determination

1. The Single Sign-on service may collect, store, and/or transmit the following checked data elements for identification and authentication services or for enrollment services. A final determination of specific data elements within the single sign-on service must wait until detailed design.

##### **Data Elements with Privacy/Confidentiality Implications**

|   |  |  |   |   |
|---|--|--|---|---|
| <input checked="" type="checkbox"/> Name  | <input checked="" type="checkbox"/> Street Address   | <input type="checkbox"/> Age                                 | <input type="checkbox"/> Occupation   | <input type="checkbox"/> IP Address   |
| <input checked="" type="checkbox"/> Social Security Number  | <input checked="" type="checkbox"/> State/City/Zip   | <input checked="" type="checkbox"/> Birth date               | <input type="checkbox"/> Marital Status   | <input type="checkbox"/> Log Records  |
| <input checked="" type="checkbox"/> Email Address   | <input type="checkbox"/> Home Phone Number           | <input type="checkbox"/> Gender                              | <input type="checkbox"/> Buying habits  | <input type="checkbox"/> Web Navigational habits  |
| <input checked="" type="checkbox"/> User Name   | <input type="checkbox"/> Work Phone Number           | <input checked="" type="checkbox"/> Authentication Q&A       | <input type="checkbox"/> Driver's License Number/State  | <input type="checkbox"/> Vehicle Serial Number  |
|   | <input checked="" type="checkbox"/> Fax Number       | <input type="checkbox"/> Photograph                          | <input type="checkbox"/> Information that identifies an individual's trade union associations | <input type="checkbox"/> Information that identifies an individual's professional associations                |
| <input type="checkbox"/> Personnel records  | <input type="checkbox"/> Finger Prints               | <input type="checkbox"/> Employee Title (position)           | <input type="checkbox"/> Information that identifies an individual's religious organizations  | <input type="checkbox"/> Information that identifies an individual's association with political organizations |
| <input type="checkbox"/> Externally obtained demographics-information acquired from external sources that describe or imply gender, age, or buying patterns |  |  | <input checked="" type="checkbox"/> Customer-obtained demographics                            |   |
| <input type="checkbox"/> Credit Card Account Number   | <input type="checkbox"/> Bank Transit Routing Number | <input type="checkbox"/> Bill Payee Name/Type                | <input type="checkbox"/> Bill Payee Address   | <input type="checkbox"/> Bill Payee Telephone   |
| <input type="checkbox"/> Bill Payee Account Number  | <input type="checkbox"/> Bank Account Number         | <input type="checkbox"/> Internal Agency Rules and Practices | <input type="checkbox"/> Trade secrets/proprietary information                                | <input type="checkbox"/> FSA maintained financial data  |

|   |   |   |   |                                      |
|---|---|---|---|--------------------------------------|
| <input type="checkbox"/> National Security Related  | <input type="checkbox"/> Communications that are protected by legal privileges <sup>1</sup> | <input type="checkbox"/> Information compiled for law enforcement purposes                |   |                                      |
| <input type="checkbox"/> Restricted Medical Records | <input type="checkbox"/> Administrative Medical Records                                     | <input type="checkbox"/> Office of Workers' Compensation Programs-Related Medical Records | <input type="checkbox"/> Employment Applicant Medical Information |                                      |
| <input type="checkbox"/> Other _____                | <input type="checkbox"/> Other _____  | <input type="checkbox"/> Other _____  | <input type="checkbox"/> Other _____                              | <input type="checkbox"/> Other _____ |

1a) The data above pertains to the following types of persons.

- Customer (Student, School Staff, Financial Partner Staff)
- FSA Employee/Contractor
- Other \_\_\_\_\_

2. The following types of individuals will have access to this data.

- Customer
- FSA Employees
- FSA Managers
- Contracted Developers
- Subcontractors
- Customer Care Representative
- Operating Partners
- Other \_\_\_\_\_

3. The source of this data are the following:

- Customer
- FSA Employee
- Operating Partners
- Other government agency
- Law enforcement agency
- Other \_\_\_\_\_

<sup>1</sup> Such as the deliberate process privilege, attorney-client privilege, and attorney work doctrine.

4. Are cookies<sup>2</sup> used (or will cookies be used)?

No       Yes (if yes, answer 4a)

4.a) What type of cookies are used?

Session cookies<sup>3</sup>       Persistent<sup>4</sup>

5. Are any of the following types of information collected? Check all that apply.

Computer content information – words or expressions contained in the body of a communication (e.g. email communications).

Computer navigation and clickstream – data passively generated by browsing the Web site (e.g. pages visited, length of time spent on Websites)

Computer interactive data - data actively generated from or reflecting explicit interactions with service providers via its Web site.

6. What are the consequences of unauthorized disclosure or misuse of this information? Check one.

Unauthorized information disclosure has no impact on FSA operations or public image

Unauthorized disclosure or misuse of the information may result in a minimal or temporary negative impact on FSA operations or public image

Unauthorized disclosure or misuse of the information would result in a significant negative impact on FSA operations or public image

Unauthorized disclosure or misuse of the information would result in a severe negative impact on FSA operations or public image

7. Is the data subject to potential fraud or manipulation for financial gain?

Information has no potential to be used for financial gain through fraud or manipulation

Information has minor potential to be used for financial gain through fraud or manipulation

Information has significant potential to be used for financial gain through fraud or manipulation

Information has high potential to be used for financial gain through fraud or manipulation

8. What is the financial impact on FSA of unauthorized disclosure or misuse of the information?

Unauthorized disclosure or misuse of the information would result in no financial loss

Unauthorized disclosure or misuse of the information would result in minor financial loss

Unauthorized disclosure or misuse of the information would result in a major financial loss

Unauthorized disclosure or misuse of the information would result in severe financial loss

9. What is the impact on the individual on whom information is maintained if unauthorized disclosure or misuse of information occurs?

No harm, embarrassment, inconvenience, or unfairness to the individual

Results in minor harm, embarrassment, inconvenience, or unfairness to the individual

Results in significant harm, embarrassment, inconvenience, or unfairness to the individual

Results in extreme harm, embarrassment, inconvenience, or unfairness to the individual

---

<sup>2</sup> Cookies are small text files that a website can place on a user's system to facilitate customer interaction with a website or for tracking purposes (to track demographic information or to track what sites a user visits).

<sup>3</sup> Session cookies are stored in the memory of a user's browser temporarily until all browser windows are closed.

<sup>4</sup> Persistent cookies are stored on a user's hard disk for a set period of time even after all browser windows are closed.

10. Is data to be retrieved by a name, unique symbol (for example, any of the data elements listed in question number 1), or other identifying element assigned to an individual?

No

Yes (if FSA PIN credentials are used for students or other users)

11. Are you providing a financial service (other than collecting a credit card number from an individual)?

No

Yes

12. Is the system collecting and storing personal health information from customers?

No

Yes

## **PART II: Privacy Compliance**

The purpose of this assessment is to determine the compliance of the Single Sign-on service with various privacy regulations.

### **The Privacy Act of 1974**

The Privacy Act of 1974 places limitations on the collection, use, and dissemination of personally identifiable information maintained by an agency about an individual and contained in an agency's System of Records (a group of records under the control of an agency from which information is to be retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. Disclosure of the information requires the prior consent of the individual (with some exceptions). [The Privacy Act of 1974](#)

- 1) Is personal data, that could identify an individual, to be retrieved by a name, unique symbol (for example, any of the data elements listed in Part I, question number 1), or other identifying element assigned to the individual?

No (skip 1a-1f)

Yes, the Privacy Act applies (answer 1a – 1f)

- 1a) Is this a new system of records?

No

Yes

I don't know

- 1b) Name the System of Records you are using (consult the Privacy Office if a new system of records is needed or to modify an existing system).

FSA Single Sign-On Service \_\_\_\_\_

- 1c) When is the new system or system modification expected to be operational?  
(mm/dd/yyyy)

12/31/2002 \_\_\_\_\_

- 1d) If a customer is asked to supply information about himself/herself, the Privacy Act notice must advise the customer of the following:

The authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

The principal purpose(s) for which the information is intended to be used;

The routine uses which may be made of the information

The effects on him, if any, of not providing all or any part of the requested information

Privacy Act Notice can be accessed via link from my website or is on a separate form that can be retained by the individual

- 1e) Check all boxes by which customers may access and correct, or request amendment, to their personal information?
- No procedures have been established outlining instructions for customers to correct their personal information
  - With a clear link or tab that leads to accessing information on the website
  - By providing specific written instructions on how to gain access to and correct their personal information
  - By providing a phone number for the customer to reach an FSA representative that will provide instructions
  - Other \_\_\_\_\_
- 1f) To comply with privacy regulations, steps must be taken to ensure the following (The items checked identify steps that will be planned for):
- Data is processed and maintained only for the purposes for which it was collected
  - Data is reliable for its intended use
  - Data is accurate
  - Data is complete
  - Data is current

### Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) Title V, governs the treatment of non-public personal information<sup>5</sup> about consumers by financial institutions.

- 2) Are you providing a financial service (other than collecting a credit card number)?
- No
  - Yes

### Other Compliance Issues

- 3) Are any contractors or business partners employed in the operation of the single sign-on system?
- No
  - Yes (if yes, answer 4a and provide name of organization involved: \_\_\_\_\_)
- 3a) Does the contractor access personal data to accomplish FSA purposes?
- No
  - Yes (if customer service representatives or security administrators have access to unencrypted user information for the purposes of updating user access information or enrollment information)

---

<sup>5</sup> Nonpublic personal information or personally identifiable financial information: Identifying information obtained in the process of purchasing a financial product or service, regardless of the source of the data; includes lists generated from nonpublic data, can include data collected through websites. (GLBA)

4) Will the website include external links or ad banners?

No  Yes (answer 4a)

4a) Do the banners comply with FSA web standards?

Yes  No

5) To your knowledge, is the system using technologies in ways that the FSA has not previously employed that have the capability to identify, locate, and monitor individuals (e.g. XML)?

No

If yes, specify \_\_\_\_\_

6) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No, skip 7a-7b

Yes, answer 7a-7b

7a) Will the new data be placed in the individual's record?

No  Yes  Other \_\_\_\_\_

7b) Who/what are the data sources?

Customer (must comply with Privacy Act requirements)

Tracking devices (must comply with ED/FSA Policy on Cookies/Tracking Devices)

Merging with an external database

7) Is the system collecting and storing personal health information about customers?

No

Yes

8) Will the system target, or do you have actual knowledge that you are collecting personal information from children under age 13?

No

Yes (if yes, answer 9a)

8a)  Check if you comply with the FSA policy regarding collection of information from children.

## 3.2 Sensitivity Determination

The following questions assist in providing a preliminary assessment of Data Sensitivity. Items with checkmarks may be applicable to the single sign-on service identification & authentication capability and/or the single sign-on service enrollment capability.

**1. If one or any of the following data elements are collected, apply a Sensitive classification:**

- Protected personnel information, customer or FSA employee health information
- ✓ Employee or customer SSN
- FSA Proprietary, FSA Financial, internal rules, or communications protected by legal privilege
- Unauthorized disclosure or misuse of data causes extreme or significant impact on an individual
- Unauthorized disclosure or misuse of data causes severe negative impact on ED/FSA image
- ✓ Information has high potential to be used for financial gain through fraud or manipulation
- Financial impact on FSA is severe if unauthorized disclosure or misuse of data occurs
- Information obtained from or compiled for a law enforcement agency
- National Security Related or information prohibited from disclosure by another law

**2. If one or any of the following data elements are collected, apply Controlled classification:**

- ✓ Personal information to be retrieved by a name or other identifier
- ✓ Information accessed by business partners/contractors/customer care representative
- Information obtained from business partners or consumer reporting agency
- ✓ Minor impact on individual if unauthorized disclosure or modification occurs
- Unauthorized disclosure or modification causes significant or minimal negative impact on ED/FSA image
- ✓ Information has significant or minor potential to be used for financial gain or manipulation
- Financial impact on FSA is major or minor if unauthorized disclosure or misuse of data occurs
- Significant or minor potential to be used for financial gain through fraud or manipulation
- Change of address
- ✓ Use of cookies on website
- Computer content, computer navigation and click-stream, or computer interactive information

**3. If one or any of the following data elements are collected, apply Non-Sensitive classification:**

- Customer or employee name, title, job description, salary (public record)
- Business addresses
- Information has no relationship to ED/FSA
- Information has no potential to be used for financial gain
- Unauthorized disclosure or misuse would result in no financial loss for FSA or impact an individual

There may be instances where questions will elicit answers that have a mixed classification, for example, both sensitive and business controlled. In most cases, where sensitive data elements and controlled are collected, stored, transmitted, and retrieved, the classification will be sensitive. In most

cases, where controlled and non-sensitive data elements are collected, stored, transmitted, and retrieved, the classification will be controlled.

Based on the evaluation above, the single sign-on service may be classified the following with respect to overall information privacy, confidentiality and sensitivity:

|  |   |  |
|--|---|--|
| <input type="checkbox"/> Non-Sensitive | <input type="checkbox"/> Controlled Sensitivity<br>(If FSA PIN data – SSN – is not stored in the single sign-on service.) | <input checked="" type="checkbox"/> Sensitive<br>(Assuming FSA PIN credential information – SSN, date of birth - is stored in the single sign-on service.) |
|--|---|--|

## 4 SYSTEM AVAILABILITY

The following assessments reflect the impact to FSA if the single sign-on system were to become unavailable.

### A) AFFECTS TO CUSTOMER OR EMPLOYEE LIFE, SAFETY, AND HEALTH

|                                     |                 |   |
|-------------------------------------|-----------------|---|
| <input checked="" type="checkbox"/> | No Impact       | System has no relationship to FSA customer or employee life, safety, or health.   |
| <input type="checkbox"/>            | Low Impact      | System unavailability could (although unlikely) result in injury or negatively impact the health of FSA customers or employees.                   |
| <input type="checkbox"/>            | Moderate Impact | System unavailability is likely to result in injury or negatively impact the health of FSA customers or employees.                                |
| <input type="checkbox"/>            | High Impact     | System unavailability would result in significant injury, or result in a major negative impact on health, or death of FSA customers or employees. |

### B) AFFECTS CUSTOMER OR FSA MISSION

|                                     |                 |  |
|-------------------------------------|-----------------|--|
| <input type="checkbox"/>            | No Impact       | System has no relationship to customer or FSA mission.   |
| <input checked="" type="checkbox"/> | Low Impact      | System unavailability may result in an inconvenience to customers but would not significantly impact customers or core FSA business activities.  |
| <input type="checkbox"/>            | Moderate Impact | System unavailability would have a major negative impact on customers or would halt FSA business activities but a work around is available that will provide some level of protection. |
| <input type="checkbox"/>            | High Impact     | System unavailability would have a major negative impact on customers or would halt FSA business activities and no feasible work around is available.                                  |

### C) AFFECTS PUBLIC CONFIDENCE OR IMAGE

|                                     |                 |  |
|-------------------------------------|-----------------|--|
| <input type="checkbox"/>            | No Impact       | System has no relationship to public confidence or image.  |
| <input checked="" type="checkbox"/> | Low Impact      | System unavailability may result in a minimal or temporary impact on public confidence or image.   |
| <input type="checkbox"/>            | Moderate Impact | System unavailability would result in a significant negative impact on public confidence or image. |
| <input type="checkbox"/>            | High Impact     | System unavailability would result in a severe negative impact on public confidence or image.      |

**D) AFFECTS MANAGEMENT CONTROL**

|                                     |                 |   |
|-------------------------------------|-----------------|---|
| <input checked="" type="checkbox"/> | No Impact       | System does not provide management and control information for decision-making.   |
| <input type="checkbox"/>            | Low Impact      | System unavailability may result in a loss of the management and control information for real-time decision-making but it is not significant. Other existing or alternate data is sufficient.                                       |
| <input type="checkbox"/>            | Moderate Impact | System unavailability could result in a loss of the management and control information for real-time decision-making but alternate current sources of information or workaround plans may provide information for timely decisions. |
| <input type="checkbox"/>            | High Impact     | System unavailability would result in a loss of the management and control information for real-time decision-making and there are no alternate sources of information or workaround plans.   |

**E) PROVIDES REQUIRED INPUT OR SUPPORT FOR A CRITICAL SYSTEM**

|                                     |                 |  |
|-------------------------------------|-----------------|--|
| <input type="checkbox"/>            | No Impact       | System has no relationship to a critical system.   |
| <input type="checkbox"/>            | Low Impact      | System unavailability may result in not providing the required input or support for a critical system.   |
| <input checked="" type="checkbox"/> | Moderate Impact | System unavailability could result in not providing the required input or support for a critical system but workaround plans may provide some level of protection. |
| <input type="checkbox"/>            | High Impact     | System unavailability would result in not providing the required input or support for a critical system and there are no workaround plans.                         |

## 5 RECOVERY OBJECTIVE

The recovery time objective is a budgeting consideration and is an input for the Disaster Recovery and Continuity of Operations planning. This assessment is needed for developing a recovery strategy that addresses the business needs of FSA.

### 5.1 Identification of Impacts over Time

The following analysis determines the degree of impact (No, Low, Moderate, High) incurred over time if the single sign-on service became unavailable. In determining the impact, it has been assumed that the service becomes unavailable during the busiest processing cycle (e.g., start of school semester, start of the workday, etc.).

| Impact Definitions |                 |   |
|--------------------|-----------------|---|
| <b>No</b>          | No Impact       | System unavailability has no impact on FSA operational activities.  |
| <b>L</b>           | Low Impact      | System unavailability may result in an inconvenience but would not significantly impact FSA operational activities. |
| <b>M</b>           | Moderate Impact | System unavailability would have a significant negative impact on FSA operational activities.                       |
| <b>H</b>           | High Impact     | System unavailability would severely impact FSA operational activities.   |

For each category below, the degree of impact of unavailability of the single sign-on service has been evaluated over various periods of time.

| Impact Categories   | 1 Hr | 8 Hrs | 24 Hrs | 72 Hrs | 1 Week | 1 Month |
|---|------|-------|--------|--------|--------|---------|
| Affects Public Confidence or Image  | L    | L     | L      | M      | M      | M       |
| Affects Outgoing Cash Flow (i.e., disbursements)<br>(Assumes FMS or other money management systems have been enabled for single sign-on. If not enabled, then No impact for all time periods)         | No   | No    | No     | L      | L      | M       |
| Affects Revenues (Incoming Cash Flow such as Repayments)<br>(Assumes FMS or other money management systems have been enabled for single sign-on. If not enabled, then No impact for all time periods) | No   | No    | No     | L      | L      | M       |
| Results in Additional Expenses (such as overtime, penalties, liabilities, etc.)   | No   | No    | No     | No     | L      | L       |
| Fraud or Theft Resulting from Unauthorized Use or Unavailability of the System  | No   | No    | No     | No     | No     | No      |

## 5.2 Summary of Impacts

The following table summarizes the preceding table in the appropriate unavailability interval.

| <b>Unavailability Interval</b> | <b>No Impact</b> | <b>Low Impact</b> | <b>Moderate Impact</b> | <b>High Impact</b> |
|--------------------------------|------------------|-------------------|------------------------|--------------------|
| Less than 1 Hour               | 4                | 1                 | 0                      | 0                  |
| 8 Hours                        | 4                | 1                 | 0                      | 0                  |
| 24 Hours                       | 4                | 1                 | 0                      | 0                  |
| 72 Hours                       | 2                | 2                 | 1                      | 0                  |
| 1 Week                         | 1                | 3                 | 1                      | 0                  |
| 1 Month +                      | 1                | 1                 | 3                      | 0                  |

### 5.3 Internal and External Dependencies

Systems that are dependent upon the single sign-on service for support must have plans with recovery strategies in the event the single sign-on service becomes unavailable. The table below identifies systems that may be dependent upon the single sign-on service for identification and authentication services, and for user enrollment services.

|     | <b>Name of the System</b>                  | <b>Provides Input to Single Sign On</b> | <b>Receives Support from Single Sign On</b> |
|-----|--|---|---|
| 1.  | Consistent Answers                         | Yes, possible for enrollment            | Yes, for I&A (planned)                      |
| 2.  | ezAudit                                    | No                                      | Yes, for I&A (planned)                      |
| 3.  | School Portal                              | No                                      | Yes, for I&A (planned)                      |
| 4.  | Student Portal                             | No                                      | Yes, for I&A (planned)                      |
| 5.  | Financial Partners Portal                  | No                                      | Yes, for I&A (planned)                      |
| 6.  | NSLDS II                                   | No                                      | Yes, for I&A (planned)                      |
| 7.  | Total & Permanent Disability               | No                                      | ?? tbd                                      |
| 8.  | IAOD                                       | No                                      | Yes, for I&A (planned)                      |
| 9.  | Common Servicing                           | No                                      | Yes, for I&A (planned)                      |
| 10. | Existing/Legacy Systems – to be determined | Tbd                                     | Tbd   |

## 6 SECURITY REQUIREMENTS

This section identifies threat categories, overall level of risk, and is used to identify possible mitigating security needs for the single sign-on service.

The overall level of risk posed to the single sign-on service by each threat event is determined by combining the likelihood of occurrence and level of impact/severity ratings. For example, a threat that has a High likelihood of occurrence (+) a Moderate level of impact/severity would have an overall risk level of High. The table below can be used to determine the risk level.

|                     | High Impact        | Moderate Impact    | Low Impact         |
|---------------------|--------------------|--------------------|--------------------|
| High Likelihood     | HIGH RISK<br>H     | HIGH RISK<br>H     | MODERATE RISK<br>M |
| Moderate Likelihood | HIGH RISK<br>H     | MODERATE RISK<br>M | LOW RISK<br>L      |
| Low Likelihood      | MODERATE RISK<br>M | LOW RISK<br>L      | LOW RISK<br>L      |

| Threat Categories   | Business Risk |   |   |     |
|---|---------------|---|---|-----|
|   | H             | M | L | N/A |
| <b>1. Loss of Business Services</b>                                   |               |   |   |     |
| Loss of Communications Providers (ISPs, ASPs)                         |               | ◆ |   |     |
| Loss of communications links or devices (cabling, router or a switch) |               | ◆ |   |     |
| Loss of facility  |               | ◆ |   |     |
| Failure of environmental services (HVAC, Power)                       |               |   | ◆ |     |
| Loss or damage of equipment room                                      |               |   | ◆ |     |
| Loss or damage of system  |               | ◆ |   |     |
| Unavailability of personnel (employee action or area disaster)        |               | ◆ |   |     |
| <b>2. Malfunctions Overloads or Failures</b>                          |               |   |   |     |
| Hardware  |               | ◆ |   |     |
| Operating System  |               | ◆ |   |     |
| Application   |               | ◆ |   |     |
| Security Services (Authentication, firewall)                          |               | ◆ |   |     |
| <b>3. Unforeseen Effects of Change</b>                                |               |   |   |     |

|   | <b>Business Risk</b> |  |   |  |
|---|----------------------|--|---|--|
| Failures due to the introduction of new software, hardware, procedures or personnel |                      |  | ◆ |  |

| Threat Categories  | Business Impact and Risk |   |   |     |
|--|--------------------------|---|---|-----|
|  | H                        | M | L | N/A |
| <b>4. Accidental Human Acts</b>                          |                          |   |   |     |
| Users  |                          |   | ◆ |     |
| Privileged Users (system administrators, developers)     |                          |   | ◆ |     |
| <b>5. Deliberate Human Acts</b>                          |                          |   |   |     |
| Users  |                          | ◆ |   |     |
| Privileged Users (system administrators, developers)     |                          | ◆ |   |     |
| <b>6. Access Violations</b>                              |                          |   |   |     |
| Unauthorized physical access                             |                          |   | ◆ |     |
| Unauthorized internal logical access                     |                          | ◆ |   |     |
| Unauthorized external logical access (hacking, sniffing) |                          | ◆ |   |     |
| <b>7. Malicious Code or Attacks</b>                      |                          |   |   |     |
| Computer viruses (worms, macros)                         |                          | ◆ |   |     |
| Trojan Horses\Backdoors                                  |                          | ◆ |   |     |
| <b>8. Theft</b>  |                          |   |   |     |
| Theft  |                          |   | ◆ |     |
| <b>9. Fraud</b>  |                          |   |   |     |
| Fraud  |                          |   | ◆ |     |
| <b>10. Legal Penalties</b>                               |                          |   |   |     |
| Legal penalties  |                          |   | ◆ |     |
| <b>11. Publicly Accessible Applications</b>              |                          |   |   |     |
| Publicly accessible applications                         |                          |   | ◆ |     |

## 7 ADDITIONAL RISKS

This section identifies additional Risk categories that must be addressed during the planning, development, deployment, and operations of the single sign-on service.

| <b>Risk Category</b>               | <b>Risk Description</b>  | <b>Risk Probability</b> | <b>Risk Impact</b> | <b>Management Strategy</b>  |
|------------------------------------|--|-------------------------|--------------------|---|
| Strategic                          | The risk of not implementing the Single Sign-On initiative will lead to additional logins required by users, multiple redundant enrollment processes and thereby decrease customer satisfaction with FSA services. Single Sign-On is a component of the FSA Modernization Blueprint to provide increased customer service and a single identification and authentication standard for FSA applications. An appropriate standard for identification and authentication needs to be developed. | Low                     | Medium             | Input from the Department, FSA, customers, industry groups and other Federal e-Gov initiatives will be included to ensure compatibility of the FSA single sign-on solution. |
| Organization and Change Management | A lack of central management of the identification and authentication to our systems will lead to fragmented processes and increased vulnerabilities. This enterprise service function will need to be managed centrally by FSA.   | Low                     | Low                | Appropriate recommendations will be made at the conclusion of Phase III.  |

| <b>Risk Category</b>                           | <b>Risk Description</b>   | <b>Risk Probability</b> | <b>Risk Impact</b> | <b>Management Strategy</b>  |
|--|---|-------------------------|--------------------|---|
| Project Resources (Financial, Personnel, etc.) | Within the Government, there is an increased emphasis on security requirements. This initiative provides a modernized basis for addressing security issues related to customer access to our systems. Security, Identification and Authentication, and single sign-on enabled system-specific authentication resources will be required to implement a successful solution. | Low                     | Medium             | The project team will be comprised of resources knowledgeable on security, identification and authentication and FSA systems.                       |
| Project Management                             | As with all enterprise initiatives, coordination across multiple organizations – internal to and external to FSA will be key to success. The project will need coordination across all the life cycle stages as well as resources, technology, and applicable standards.  | Low                     | Low                | An IPT (Integrated Product Team) approach will be utilized to ensure timely participation and contribution.   |
| Business                                       | Strengthening the identification, authentication and enrollment process will require close coordination with the customer community. The FSA customers will need to adopt this single sign-on solution for single login and access to FSA systems.  | Low                     | Low                | Phase III and activities will include community outreach tasks to ensure comprehensive understanding of new service.                                |
| Data/ Information                              | The fragmented access mechanisms to our systems lead to system vulnerabilities that can be controlled. Login data will be maintained within the appropriate single sign-on data store.  | Low                     | Medium             | The design of the login data store will include federal standard levels of encryption, backups for recovery and hot sites continuity of operations. |

| <b>Risk Category</b>          | <b>Risk Description</b>  | <b>Risk Probability</b> | <b>Risk Impact</b> | <b>Management Strategy</b>  |
|-------------------------------|--|-------------------------|--------------------|---|
| Application                   | A long-term vision for architecture will need to be realized across all enterprise system assets. Connectors from single sign-on to FSA systems will be required.                        | Low                     | Low                | Industry and Federal standard techniques will be utilized to implement COTS/GOTS connectors from the single sign-on facility to enabled systems.  |
| Technology/<br>Infrastructure | The single sign-on technology is maturing, the federal standards for cross-organization identification and authentication are evolving, and appropriate infrastructure will be required. | Low                     | Low                | Phase III will implement technology compatible with the evolving e-Gov e-Authentication standards, PAMs (Pluggable Authentication Modules) to support additional identification and authentication sources and the infrastructure will be scaled to handle the required capacity. |
| Security                      | Login data will be maintained within the single sign-on data store to support single login.  | Low                     | Medium             | The design of the login data store will include federal standard levels of encryption, backups for recovery and hot sites continuity of operations.   |
| Privacy                       | The Single Sign-on does not intend to store or collect privacy data. However if FSA PIN credentials are stored in the service, then SSN and date of birth will need to be stored         | Low                     | Medium             | The design of the credential data store will include federal standard levels of encryption. The sensitive data will be stored in an encrypted state. Only cleared customer service and support staff will have access to this information.  |