

***FSA Integration Partner Program***  
United States Department of Education  
Office of Federal Student Aid



**Security Architecture Status Report –  
October – November 2003**

***Deliverable #120.2.4***

***Task Order #120:  
Security and Privacy Support***

**Version 1.0**

**November 26, 2003**

### Document Revision History

Version Number	Date	Author	Revisions Made
1.0	November 26, 2003	Jesse Bowen	Initial submission

## Table of Contents

<b>1</b>	<b>EXECUTIVE SUMMARY.....</b>	<b>4</b>
<b>2</b>	<b>INTRODUCTION.....</b>	<b>5</b>
<b>3</b>	<b>SECURITY ARCHITECTURE STATUS OVERVIEW .....</b>	<b>6</b>
3.1	BACKGROUND.....	6
3.2	TASK ORDER OBJECTIVES .....	6
3.3	PROGRESS TO DATE .....	7
3.3.1	<i>Architecture Presentation to Department of Education .....</i>	<i>7</i>
3.3.2	<i>Status Meetings.....</i>	<i>8</i>
3.3.3	<i>Coordination with Data Strategy Projects .....</i>	<i>8</i>
3.3.4	<i>Coordination with e-Authentication Efforts.....</i>	<i>8</i>
<b>4</b>	<b>DATA CLASSIFICATION RECOMMENDATIONS .....</b>	<b>9</b>
4.1	INTRODUCTION.....	9
4.2	GOALS FOR DATA CLASSIFICATION .....	9
4.3	DRAFT DATA CLASSIFICATION STRUCTURE.....	9
4.4	RECOMMENDED DATA CLASSIFICATION LABELS .....	10
4.5	RECOMMENDATIONS FOR ESTABLISHING A DATA CLASSIFICATION PROCESS.....	11
4.6	DATA CLASSIFICATION PROCESS CONSIDERATIONS .....	11

# 1 Executive Summary

This document is a required deliverable for Task Order 120 – Security and Architecture Support. TO 120 provides support to FSA for a variety of security and privacy support activities. A modification of the original task order was approved in July 2003 to add activities related to security architecture to the original scope of TO 120. This document is a status report on the activities conducted during October and November of 2003, related to support of development and deployment of the FSA Security and Privacy Architecture.

This deliverable contains the following major sections:

- Security Architecture Status Overview (Section 3)
- Draft Data Classification Recommendations (Section 4)
- Draft FSA Web Security Standard Status (Attachment), containing –
  - Introduction
  - Scope and Applicability of Standard
  - FSA Web Security Standards and Guidelines
    - Security of Network and Infrastructure
    - Security of Web Servers
    - Security of Web Applications
    - Web Services Security Standards
    - Encryption for Web Components
  - Implementation Approach
  - Appendices
    - List of TCP/IP Ports to Block
    - References
    - Overview of FSA Security and Privacy Technical Architecture

## 2 Introduction

This document is a required deliverable for Task Order 120 – Security and Architecture Support. TO 120 provides support to FSA for a variety of security and privacy support activities. TO 120 was modified in July 2003 to provide additional support to continue development and communications efforts for the FSA Security and Privacy Architecture.

This document is a status report on the activities conducted during October and November of 2000 to support the development and deployment of the FSA Security and Privacy Architecture.

This deliverable contains the following major sections:

- Security Architecture Status Overview (Section 3), which summarizes activities conducted in support of the FSA Security and Privacy Architecture.
- Draft Data Classification Recommendations (Section 4), containing a proposed data classification structure and outlining processes that will be required to implement data classification processes.
- Draft FSA Web Security Standard Status, provided as a separate attachment, containing –
  - Introduction
  - Scope and Applicability of Standard
  - FSA Web Security Standards and Guidelines
    - Security of Network and Infrastructure
    - Security of Web Servers
    - Security of Web Applications
    - Web Services Security Standards
    - Encryption for Web Components
  - Implementation Approach
  - Appendices
    - List of TCP/IP Ports to Block
    - References
    - Overview of FSA Security and Privacy Technical Architecture

## 3 Security Architecture Status Overview

### 3.1 Background

FSA recently completed a project under Task Order 124 to create a Security and Privacy Architecture Framework, Specification, and Implementation Strategy<sup>1</sup>. The implementation strategy recommended several actions that will prepare FSA for development and deployment of security standards and services, and will promote understanding and adoption of the FSA Security and Privacy Architecture.

FSA defined several tasks that will support follow-on activities related to continued development of security architecture components. FSA created an SOO to define this work, and submitted it to the Integration Partner Program on June 23, 2003. The Security Architecture support activities were organized as a modification to Task Order 120 – Security and Privacy Support. A modified Technical Proposal for Task Order 120 was submitted by the Integration Partner Program on July 7, 2003. FSA accepted the modified Technical Proposal, and subsequently awarded a modification to Task Order 120 to cover the security architecture support objectives and deliverables.

### 3.2 Task Order Objectives

A new Task Area, 3.12, was added to TO 120 to cover security architecture support activities. This task area will provide half-time staffing of a Senior Security Architect to act as a security Subject Matter Expert. The security architect aided the FSA security organization with planning and delivering initial components of the security architecture. The security architecture support included specific tasks as well as *ad hoc* support for security architecture and integration questions. It also covered integration issues and activities arising from other FSA projects (such as Data Strategy and PIN Reengineering Analysis) that have security architecture implications.

The specific objectives of Task Area 3.12 were:

1. Begin preparation work for developing the FSA security architecture
  - Assist FSA with communicating the Security Architecture vision to CIO and business groups
  - Perform a gap analysis of the existing FSA IT Security and Privacy Policy to define policies and standards that will require modification or development to support the FSA Security Architecture
  - Create recommended web security guidelines
  - Recommend data classification definitions for classifying the sensitivity of FSA data
  - Provide general security architecture support, such as attending *ad hoc* meetings and advising FSA as a security subject matter expert
2. Support system risk assessments and Certification & Accreditation activities
  - Assist preparation of up to four Tier 2 systems for Certification & Accreditation
    - Tier 2 systems in scope may include PGA, LMS, IFAP, and eCB

---

<sup>1</sup> Task Order Deliverables 124.1.1, 124.1.2, and 124.1.3

- Assess any additional information needed to prepare for C&A
- Work with SSOs for the systems to prepare C&A documentation
- Support risk assessment of the Disability Discharge Tracking System (CDDTS)

### **3.3 Progress to Date**

Previous status reports<sup>2</sup> have covered activities between June and September 2003, including the policy gap analysis, the security risk assessment for CDDTS, and communications activities as described in the Task Order Objectives above.

Activities in support of the FSA Security and Privacy Architecture conducted during October and November 2003 are described below.

#### **3.3.1 Architecture Presentation to Department of Education**

The FSA Security and Privacy Architecture was presented to representatives of the Department of Education on October 27, 2003. The goal was to provide an overview of the FSA security framework to Dept. Education personnel and contractors who are coordinating Enterprise Architecture and Security Architecture efforts.

In attendance at the meeting were:

- Nina Aten (Dept. Education)
- Arthur Graham (Dept. Education) – Enterprise Architecture
- Joe Rose (Dept. Education) – Enterprise Architecture
- John Dodd (CSC) – Contractor to Dept. Education for Enterprise Architecture Support
- Bob Ingwalson (FSA) – Computer Security Officer
- Jesse Bowen (Accenture) – Contractor to FSA for Security Architecture Support

An overview of the FSA Security and Privacy Architecture was provided, followed by discussion of how the FSA security framework could be integrated with Dept. Education Enterprise Architecture efforts.

The FSA Security and Privacy Architecture was also discussed at a meeting of the Department of Education Architecture Working Group on November 5, 2003. The overall goal of the meeting was to discuss the Department of Education approach for Security Architecture. As part of that discussion, the FSA Security and Privacy Architecture was addressed as an example of a Technical Reference Model to support development of Security and Privacy Profiles.

---

<sup>2</sup> Task Order 120 Deliverables 120.2.1, 120.2.2, and 120.2.3.

### **3.3.2 Status Meetings**

Weekly status meetings were conducted during the reporting period with Bob Ingwalson, the FSA Computer Security Officer. These status meetings reviewed work in progress, provided an opportunity for planning upcoming activities, and communicated progress on other task orders that affect implementation of the FSA Security and Privacy Architecture.

### **3.3.3 Coordination with Data Strategy Projects**

The FSA Security and Privacy Architecture was integrated into deliverables created for the Data Strategy project. The Data Strategy effort is designed to define several aspects of the long-term vision for the methods FSA will use to structure and process business data critical for FSA business operations. The following list summarizes progress in communicating and integrating the FSA Security and Privacy Architecture into various Data Strategy deliverables.

- **Technical Strategies** – the FSA Security and Privacy Architecture was referenced by the Technical Strategies deliverables as a framework for providing security services to FSA internal and external information systems. The Technical Strategies deliverable defined the alignment of security for Web services with the Web Services Security layer of the FSA Security and Privacy Architecture framework.
- **Enrollment and Access Management** – the FSA Security and Privacy Architecture was used as a framework to develop a conceptual vision of how FSA will provide access management and identity management services for FSA trading partners<sup>3</sup>. The conceptual vision for Enrollment and Access Management was aligned with the Access Management layer, to provide authentication, single sign-on, and access control services, and with the Identity Management layers to provide user provisioning, administration, and password management services.

### **3.3.4 Coordination with e-Authentication Efforts**

Discussions with the FSA e-Authentication project were held to clarify how FSA could participate in the GSA e-Authentication program. These meetings included Charlie Colman and Neil Sattler from FSA. Two external meetings were also attended to discuss pilot projects, one with Educause and the Department of Health and Human Services, and the other with Steve Timchak, GSA Project Manager for e-Authentication.

Recent developments in the GSA e-Authentication program have resulted in a change of focus away from developing a single authentication gateway. The new goal of the program is to establishing guidelines for use of federated identity standards based on the Liberty Alliance and the SAML specifications for communicating authentication credentials and access control information.

---

<sup>3</sup> See Appendix D of Deliverable 123.1.29.

## **4 Data Classification Recommendations**

### **4.1 Introduction**

When making decisions about the level of security required for an FSA system or application, the type of data stored or processed by the system is often considered. Currently, there is no standard structure available to assign security classes to FSA data. As a result, decisions based on the type of data rely on the knowledge of FSA personnel or their contractors to define the sensitivity level of specific forms of data. This may produce inconsistent decisions about the level of security required, and is open to challenge when disputes arise about the security controls that should be implemented for specific types of data. A standard data classification structure and a data classification process will help FSA make such decisions in a more consistent and timely manner. The data classification structure and recommendations in this section provide a starting point for development of a data classification process.

Data classification is a formalized decision process that assigns labels to data to establish its sensitivity level. Data classification labels can help define security controls that are applied to data as it is created, modified, stored, or transmitted. The sections below define a proposed data classification structure for FSA. Critical to successful use of a data classification scheme, however, are the processes defined to implement a data classification process. An overview of the processes that will need to be defined and established is also presented to provide practical recommendations on an implementation approach for data classification.

Some of the guidance discussed below is based on ANSI standards<sup>4</sup>

### **4.2 Goals for Data Classification**

The major goals for establishing data classification structure discussed below is to:

- Provide input to decisions about required security controls for different data classes.
- Help FSA and its contractors determine when data should be encrypted, either during transmission or when stored.
- Define standard processes for assigning and modifying data classification labels to data.

### **4.3 Draft Data Classification Structure**

At a high level, the following types of data may be stored, processed, or transmitted by FSA systems and applications:

- Personal and private data – information about borrowers, including personal, financial, and (in disability discharge systems) medical information.

---

<sup>4</sup> ANSI Standard A/I 11179, Information Technology - Specification and standardization of data elements - Part 2: Classification for data elements.

- Financial data – FSA processes financial data about individuals and institutions. Some financial data may be aggregated, in the form of “metadata” about finances, shared with the Treasury Department
- Information about FSA security – credential information, configuration data, security procedures, risk assessments, vulnerabilities, etc.
- FSA internal information – strategic information, data about FSA internal operations.
- Employee data – information about FSA employees or contractors.
- Eligibility data for institutions.
- Information about services provided by FSA.
- Public information – typically, public information is not sensitive, although FSA may desire that public information displayed by FSA systems is correct and cannot be altered.

#### **4.4 Recommended Data Classification Labels**

Data classification labeling schemes typically work best when the following criteria are satisfied:

- The number of data classes is minimized.
- The data classes are distinct and mutually exclusive.
- The data classes collectively encompass all the types of data stored or processed by the organization.
- Criteria for each data class are clearly defined in a way that promotes efficient data labeling.

FSA data can be generally divided into five primary areas, as described below.

<b>Personal</b>	personal information about individuals that may subject to Privacy Act protections, very sensitive
<b>Individual Financial</b>	financial data about individuals, including income, tax information, financial assets, etc.
<b>Financial</b>	information about FSA financial operations, such as integrity data; financial transaction information, payment information, etc.
<b>Operational</b>	data about FSA operations of a less sensitive nature than financial information, dealing with data about FSA, schools, lenders, and other trading partners.
<b>Public</b>	non-sensitive data that can be freely provided to the public without restrictions.

These five areas could be used as the basis for developing the data classification processes defined in the following sections. Additional criteria should be developed to

formally define and discriminate between these data classes as the data classification process is designed.

#### **4.5 Recommendations for Establishing a Data Classification Process**

To implement a data classification system, FSA will need to establish several processes, define responsibilities for each process, and develop the appropriate governance and oversight mechanisms. The list below briefly defines the major tasks and processes required to support a data classification scheme.

- Establish information classification criteria – define the basic data classification labels, criteria for determining which labels apply to various data types, and methods for documenting data classification decisions.
- Establish a data classification policy – an addendum to the FSA IT Security and Privacy policy should be created to document the FSA data classification scheme and define the high-level responsibilities for implementing and monitoring its effectiveness.
- Classify and label existing data – a process will be needed to retroactively label existing FSA data. Alternatively, FSA could decide to only apply data classification labels to new systems, or as the need arises during system design, development of System Security Plans, or when Certification and Accreditation are being conducted.
- Classify and label new information – design, develop, and document processes to follow to assign data classification labels to new data. The process design should include definition of responsibilities for each step.
- Establish information 'ownership' criteria – one approach to classifying data is to assign data owners responsible for making decisions about specific data sets. If FSA adopts this approach, criteria should be developed to define the responsibilities of data owners and the steps they should follow when classifying data.

#### **4.6 Data Classification Process Considerations**

During development of data classification processes, the following issues are representative of the major design considerations that will need to be addressed.

- How to handle appeals or disagreements that may arise about assignment of the appropriate classification labels for specific types of data.
- Changing classification data when requirements, policies change, or data is rendered non-identifiable.

- Classifying new types of data or data that will be stored or processed by new FSA systems and applications.
- How to define data classification labels and requirements for test data.
- How to handle classification of mixed types of data.
- Who is responsible for monitoring data classification processes.
- How data classification definitions and criteria will be reviewed and updated.