

eMPN Security Risk Assessment Results
Task Order 65 – Deliverable 65.1.2
E-Sign Mad Dog

The purpose of the Risk Assessment and System Security Review was to understand the security environment within which the eMPN process would operate. The approach to address this deliverable changed paths numerous times throughout the duration of the effort. As the eMPN project transitioned through its lifecycle stages, we became cognizant of the need to pursue a more direct approach to acquire the necessary security and risk information. The bulleted list below describes the process we followed to obtain the information on the following pages. The final product is a sound, thorough examination of the eMPN website. While further effort is necessary to ensure the contractors involved understand their role in securing the eMPN process, the current documentation sufficiently describes the environment within which the eMPN will operate.

- To kickoff the effort, we began interviewing several key SFA personnel about the future eMPN process. This effort produced a baseline understanding of eMPN and its basic structure. However, it did not produce the level of detail we needed to assess the security risks of the application. Therefore, we redirected our efforts to the contractors supporting the SFA personnel. At this early stage in the design process, the contractors did not have a clear assessment of the security risks that may affect the eMPN.
- After pursuing numerous leads toward security information to little avail, we were instructed by the LO lead, Rosemary Beavers, to give LO and their contractor, EDS, the exact information we required for our security risk assessment. At this point, we studied SFA's Certification and Accreditation process and found the basis for our response to LO. Although SFA's C&A program is not fully defined and no system in SFA has gone through the C&A process, we decided to take a step towards beginning a C&A program.
- We created a framework to elicit answers from LO and their contractor, EDS. The framework provided a series of questions relating to specific security controls that EDS would employ to mitigate security risks present within the eMPN process. We delivered the framework, through Andy Boots, SFA's Computer Security Officer, to Don Dorsey, System Security Officer for LO/LC, and Don in turn delivered the document to EDS. The results of that effort comprise the remainder of this deliverable. While the path to success was circuitous and oftentimes difficult, the final deliverable makes a dramatic push towards understanding the security risks with eMPN, created security/risk documentation to present at the Production Readiness Review, and had the ancillary benefit of launching the C&A program within SFA.

System Security Review Worksheet ePN Server

Note: The security of the ePN website depends on several different elements working together. This security review worksheet includes both the security controls that fall under EDS' direct scope of responsibility, as well as security controls implemented and managed by CSC and NCS. EDS' scope of responsibility is that which resides within the website application. To understand the totality of security controls and the impact on the Loan Origination Subsystem (LOS), it will be necessary to obtain security information from the contractors that are responsible for other components of the LOS program, CSC and NCS. Specifically, information regarding operating system security and the network and physical security of the web servers in question will be required.

1. INTRODUCTION AND SUMMARY

Briefly describe the system and its business function.

The LOS was developed to support the Department of Education's William D. Ford Federal Direct Loan Program. This program's purpose is to provide direct loans to students for their education.

The Loan Origination Subsystem (LOS) Electronic Promissory Note (ePN) provides borrowers participating in the William D. Ford Federal Direct Loan Program with the ability to create, store, and retrieve master promissory notes for all Direct Subsidized and Unsubsidized loans.

The ePN system is comprised of a web and application server and the Promissory Note database server. Borrowers wishing to complete an ePN participate in a three-stage process beginning with authentication, followed by disclosure and acknowledgement, and finally submission of the signed ePN. Borrowers wishing to retrieve one of their ePN's complete a two-stage process beginning with authentication and then retrieval and display of ePN data and PDF files.

2. BACKGROUND

Provide contextual information for the Designated Approving Authority (DAA). Identify the security standards or policies applied to the system.

DAA: Department of Education, Kay Jacks

Student Financial Assistance Chief Information Officer: Andy Boots

Student Financial Assistance Office

Direct Loan Origination: Don Dorsey

Loan Consolidation: Yvette Payne

Contracting Officer's Technical Representatives:

Loan Origination (LO): Steve Wingard

Loan Consolidation (LC): Fred Haynes

SECURITY STANDARDS

Privacy Act of 1974 – Public Law (PL) 93-579

Freedom of Information Act – PL 93-502

Federal Managers' Financial and Abuse Act of 1983 – Federal Law (FL) 97-n 225

The Computer Fraud and Abuse Act of 1986 – FL 99-474

The Computer Security Act – FL 100-235

OMB Circular No. A-130 Appendix III, Security of Federal Automated Information Systems

OMB Circular No. A-127 Financial Management Systems

OMB Circular No. A-123 Internal Control Systems

OMB Bulletin No. 90-08 Guidance for Preparation of Security Plans for Federal Computer Systems that contain Sensitive Information

US Department of Education, Office of Post Secondary Education, Information Technology Security Manual, Handbook 6, Nov. 14, 1994

FIPS PUB 11 Dictionary of Information Processing

FIPS PUB 38 Guidelines for Documentation of Computer Programs and Automated Data Systems

FIPS PUB 41 Computer Security Guidelines for Implementing the Privacy Act of 1974

FIPS PUB 73 Guidelines for Security of Computer Applications

Department of Education Standards for Electronic Signatures and Electronic Student Loan Transactions

2.1 System Name

Identify the system as it is or will be described in a system security plan.

The following are new components of the LOS. The application security for which EDS has responsibility will be described in two addenda to the CSC Security Plan, one for LO and one for LC.

ePN Web Server

ePN Database Server

2.2 System Description

Describe the system as a major application, general support system, minor application, etc as explained in OMB A-130 Appendix III. However, if you consider ePN an addition to the DLO system, explain this here.

2.2.1 GENERAL SUPPORT SYSTEM

This is an addition to the LOS, since it adds additional functionality to an already existing system.

The ePN Web Server falls under the same direct hardware, network, and operating system control as the LO/LC Webservers, which are administrated by CSC. The ePN websites share common functionality with the LO/LC Websites as they provide the end user with information pertaining to the user's Loan Origination and Loan Consolidation information, and add the option for the end user to electronically sign her or his P-Note. EDS' responsibility concerning security controls is limited to the application layer processes of the websites.

Also, rate the system as high, moderate, low or negligible risk for electronic authentication. These ratings are defined by the Department of Treasury Electronic Authentication Policy dated January 3, 2001. (See appendix A.)

The system is rated as low risk for electronic authentication purposes. The potential risk of the system was assessed based on the elements indicated in the Department of Treasury Electronic Authentication Policy, found at Appendix A: The risk of monetary loss, reputation, and productivity. Because the risk is low, at a minimum, single-factor authentication must be used.

EDS understands the authentication process as it stated below, based on the contractual framework of the LOS, the requirements document and direct input from management. However, this process is managed, administered and secured by contractors other than EDS, so it is advised that the other contractors be consulted on the process. Robust authentication has been built into the ePN as specified below. The process meets the basic requirements for single-factor authentication, and adds significant additional security controls that make the authentication even stronger than is required.

2.2.2 AUTHENTICATION PROCESS

The process is as follows:

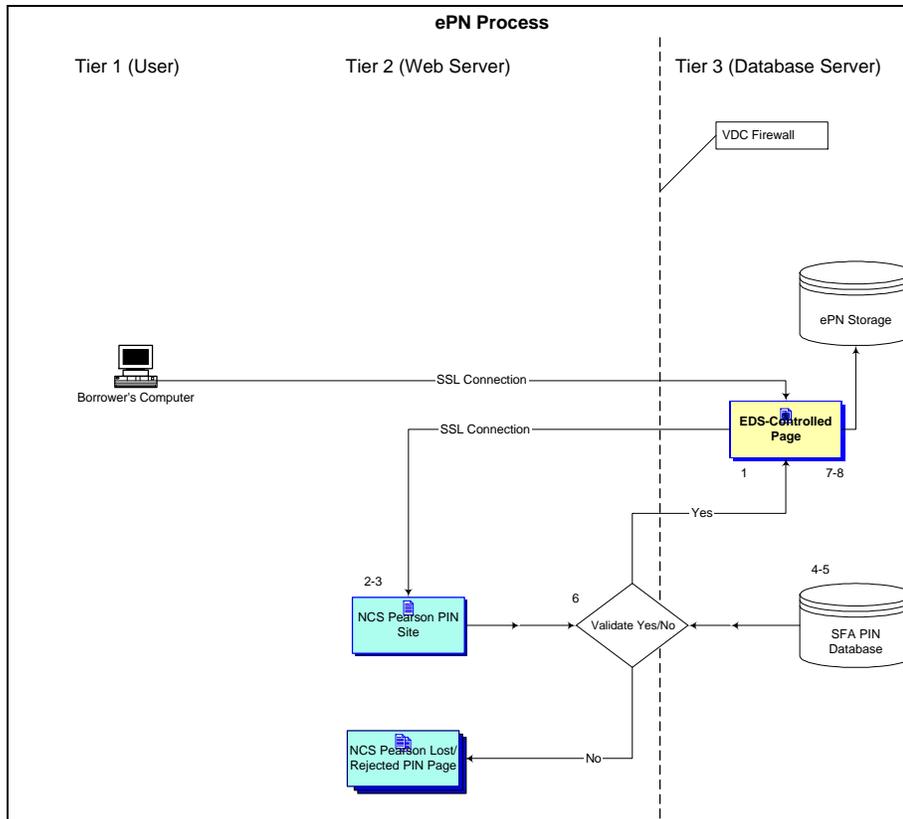
- 1. The user goes to the ePN website, maintained by EDS.**
- 2. The user is redirected to the PIN site, maintained by NCS.**
- 3. The user enters in authentication information: the user's PIN, Social Security Number and date of birth.**
- 4. The information is sent by encrypted secure communication (SSL) to the School Financial Assistance (SFA) PIN Database.**
- 5. It is validated at this site, behind the VDC firewall.**
- 6. If the information is validated, the information is sent back, encrypted over SSL, to the PIN website. (If the information is not validated, the user is redirected to the bad pin website, which is controlled by NCS.)**
- 7. The PIN website then allows the user to continue forward onto the ePN website, encrypted, by SSL on Port 443.**
- 8. The user is then able to create and sign an electronic promissory note on the ePN website.**

2.3 System Boundary

Describe the system by defining the boundaries around a set of processes, communication, storage, and related resources (architecture). This section should identify the points at which your system interfaces with another system not under your control. Also include security assumptions about areas and actions outside the boundaries (i.e. students, schools,).

EDS is responsible for the security residing within the application layer. EDS is not responsible for developing and maintaining the hardware and network architecture. Therefore, we are unable to describe the system. For a description of the system architecture, please contact CSC.

We have developed the diagram on the next page that defines the ePN system as we understand it, and which shows EDS' place within the ePN system. It shows where the system interfaces with other systems not under our control, by defining a logical mapping of the path a user's request for access follows.



- THE USER GOES TO THE ePN WEBSITE, MAINTAINED BY EDS.
- THE USER IS REDIRECTED TO THE PIN SITE, MAINTAINED BY NCS.
- THE USER ENTERS IN AUTHENTICATION INFORMATION: THE USER'S PIN, SOCIAL SECURITY NUMBER AND DATE OF BIRTH.
- THE INFORMATION IS SENT BY ENCRYPTED SECURE COMMUNICATION (SSL) TO THE SCHOOL FINANCIAL AID (SFA) PIN DATABASE.
- IT IS VALIDATED AT THIS SITE, BEHIND THE VDC FIREWALL.
- IF THE INFORMATION IS VALIDATED, THE INFORMATION IS SENT BACK, ENCRYPTED OVER SSL, TO THE PIN WEBSITE. (IF THE INFORMATION IS NOT VALIDATED, THE USER IS REDIRECTED TO THE BAD PIN WEBSITE, WHICH IS CONTROLLED BY NCS.
- THE PIN WEBSITE THEN ALLOWS THE USER TO CONTINUE FORWARD ONTO THE ePN WEBSITE, ENCRYPTED, BY SSL ON PORT 443.
- THE USER IS THEN ABLE TO CREATE AND SIGN AN ELECTRONIC PROMISSORY NOTE ON THE ePN WEBSITE.

We cannot make any specific assumptions about controls outside of the scope of EDS' responsibility, such as students or schools, because they are not under the EDS purview. Nor can we make such assumptions regarding the PIN aspect of authentication, since it is under the control of NCS and CSC.

2.4 System Components

Describe all hardware and software used to operate to operate the system. Also, describe all connections with supporting systems. Include a textual description and an architecture diagram. Specifically identify any new components needed for the ePN. Identify formal agreements with service providers (e.g., VDC) or partners (e.g., schools, guarantee agencies) that support system operation.

The ePN Web Server will be operating on a “HP L Class Server”, running the HP-UX 11 Operating System with 2 Processors and 5 gig of RAM. The web application runs on a Netscape server.

The ePN Database Server will be operating on a “HP T Class Server”and running the HP-UX 10.02 Operating System, with 10 Processors and 2 gig of RAM. The DBMS is Informix.

The system resides in the Virtual Data Center (VDC) in Meriden, Connecticut, which is controlled by CSC. The architecture, and system components related to other such hardware and software, are outside of the control of EDS, and cannot be described here.

EDS controls the LO/LC Website applications on the web servers (CSC controls the actual servers, network and firewall), as well as the Database Server. (CSC controls the operating system, physical environment, network and firewall).

EDS does not have any trading partner agreements with either CSC or NCS at this time.

3. SECURITY AND RISK

Additional security risk based on changes/modifications/additions

Identify any additional security risk resulting from the changes/modifications/additions to the system (Refer to section 2.4).

There are a few additional security risks resulting from the addition of the new system components, although most of them can be significantly mitigated as discussed in section 3.1.

- **All of the system components have been divided over three different contractors. This splitting of security management among three different contractors without executing a formal agreement as to security standardization within the entire system is a risk.**
- **The PIN server is placed outside the VDC firewall, and the network path that users' data follow during the authentication process passes through CSC's firewall and other network servers/connections multiple times.**
- **SSL has been added to the system to allow encrypted communication between the end user and the ePN servers. SSL communicates through a well-known standardized port. Since this port is commonly used as a communication port within SSL, it potentially opens up a security hole through which wrongdoers could pass.**
- **An imposter could attempt to sign the promissory note.**
- **Unauthorized individuals may attempt to alter promissory note data.**
- **The signer could later attempt to deny signing the promissory note, and EDS or the Department could deny receiving the promissory note.**
- **Unauthorized individuals could attempt to view sensitive information.**

There may be additional risks found on the components under the control and management of CSC and NCS.

3.1 Security Controls

Summarize the controls that are in place currently and their general roles in protecting assets against threats and preventing exposures. Also, describe new security controls employed/ to be employed to mitigate additional risk (if necessary).

EDS understands the security controls described below are those that are in place, based on the contractual framework of the LOS, the requirements document and direct input from management. These are controls that have been put in place to mitigate the risks identified in section 3. Many of the factors indicated below are under the control and management of CSC or NCS, and EDS cannot confirm that they are operational. CSC and NCS must obtain verification and validation of the security controls stated.

Electronic Promissory Note (ePN) records are protected from unauthorized access in several ways.

- **Strong (128-bit) authentication is used to prevent imposters from signing the promissory note, and to prevent the signer from later attempting to deny signing the promissory note.**
- **Strong authentication combined with DES encryption piped through an SSL connection is used to prevent unauthorized persons from accessing sensitive information.**
- **ePN records are stored on a separate database server, in a separate database, from the Loan Origination and Loan Consolidation database. At the time the ePN record is created, the appropriate promissory note data is simultaneously written to the appropriate tables in the LO or LC database limiting the need to retrieve information from the ePN database.**
- **Applications interfacing with the ePN database restrict the records that can be viewed by users.**
- **The server and database used to host the ePN databases restrict direct access to the ePN database to authorized users only.**
- **The ePN record contains demographic data, event data, authentication data and a Portable Document Format (pdf) file. Upon submittal of the signed ePN by an authenticated borrower, the system merges demographic and event related data into the pdf, generates an MD5 hash code for the merged pdf, and stores the pdf, hash code and appropriate data to the ePN database. The hash result will show if the file has been manipulated. Hash results will only be monitored if it is suspected that the file has been modified, for example in the case of repudiation of the information on the file. The hash functions will be applied to the pdf files for both LO and LC.**
- **The system provides assurance through the PIN site authentication process. The ePN and LC Application Entry applications obtain authentication information from the NCS PIN site, a trusted source outside of the Department of Education (ED) firewall, and therefore outside of ED's and EDS' control. The PIN site verifies the PIN with the SFA PIN database through a secure (SSL) connection.**
- **Access to the ePN records is controlled on several levels.**
 - **For the database security: first, UNIX security, on the database server, provides the ability of the system administrator to assign/adjust access level privileges at the server level. Second, the Informix database controls the rights that users are granted to access ePN records. Third, the applications interfacing with the ePN database control the type of access a user is granted based on role.**

- For the ePN application, the borrower may insert or retrieve only ePN records pertaining to them.
 - For the LO and LC websites, the security administrator will control the level of access granted to a particular user role. Only selected user roles will be able to retrieve PDF files.
- A session will be created for each borrower accessing the ePN or Application Entry website. Borrower information and transaction data obtained during the ePN process will be retained on the session in memory. A session cookie will be placed on the borrower's computer hard-drive to allow for submissions to be associated with the correct session. The session data will be removed following termination of the session. The session cookie information will be cleaned up when the borrower exits her or his browser.
- Upon final review and acceptance of the ePN by the borrower, the session data will be merged into the pdf file and a MD5 hash code developed. The resulting ePN record including the pdf file will be inserted into the ePN database.
- The electronic signature is a process, made up of the authentication, acknowledgement of the legal impacts of clicking the button that signs the document, as well as multiple screens before submitting the P-note to the database that give the user a chance to review the document.
- The user is authenticated with their full name, social security number, and PIN through NCS' PIN website. The captured session events and information related to what transpired during the session are retained as part of the pdf file that is retained in the ePN record. The MD5 hash code computed for the pdf file provides assurance that the pdf has not been modified once saved. At the systems level, UNIX security provides access controls to determine what level of access a user has to the server and Informix database. At the application level, the appropriate security component limits users' access to ePN records and what tasks can be performed. This level of access is tied to the user role and login id.
- Key process transactions are retained on the session. Upon acceptance of the Promissory Note terms and conditions, these transactions are merged into the pdf file, which becomes the authoritative copy of the ePN. The web server also writes application transactions to a log file that is reviewed by production support personnel. The Web Trends reporting tool is used to prepare daily and weekly reports on web events.
- The encryption algorithms used by the STAN (PIN) site are DES password-based and use symmetric encryption. NCS Pearson has developed code in C/C++ and Java using RSA Bsafe and Baltimore Keytools cryptography packages.
- Verisign technology (not PKI digital signatures) will also be used on both the LO and LC ePN/e-signature sites for authentication and confidentiality purposes. This helps prevent unauthorized access, as well as helps to insure the identity of the user. The ePN server utilizes VeriSign Server Ids. These ids or digital certificates allow servers so equipped to communicate with the Microsoft and Netscape client-side browsers using secure socket layer (SSL) encryption.

3.2 Residual Risk

Describe any risk that will not be mitigated. Any residual risk should be explicitly accepted or declined by management.

There are several risks identified in section 3 that have not been entirely mitigated.

- **As EDS' control over the ePN system is limited to application security, we are unable to mitigate any risks that arise from the components outside of our authority.**
- **The splitting of security management among three different contractors without executing a formal agreement as to security standardization within the entire system.**
- **The PIN server is placed outside the firewall, and the users' authentication information passes through CSC's firewall and other network servers/connections multiple times.**
- **Using a well-known SSL port for communication between the end user and the ePN servers.**
- **All physical, operational and network security is not under EDS' control.**

3.3 Specific Changes to Security Plan (Listed by section number)

Determine how you will document your security controls. Do you plan to update an existing security plan or write a new security plan? If the changes are to an existing security plan, identify each modification specifically by section number and heading. Also, include an intended date for these changes to be made. If you plan to write a new security plan, identify an estimated completion date, or if completed, attach to this document.

EDS is drafting Addenda to the current CSC Security Plan for the LC and LO websites that will include all application level controls associated with ePN. CSC's security plan must be taken into consideration when reviewing the addenda. Modifications will be made with regard to all significant security elements of the ePN. The Addenda will be completed on or about June 28th, 2001.

Additionally, the LOS System Security Plan will be updated as needed, throughout the life of the LOS.

3.4 Corrective Action Plan

If, after this review, you need to correct security controls to mitigate risk, prepare a corrective action plan with dates and responsible party.

Appendix B outlines the areas of concern that have been identified in past security assessments as needing corrective action. Although the corrective action items address the security system as a whole, specific attention should be given to how they may affect the security of the ePN websites addressed by this questionnaire, once the website are on-line and fully operational.

EDS also suggests that the Department review the system with regard to the splitting of security management among three different contractors to determine if this framework best mitigates the risks associated with the LOS.

A trading partner agreement should be established EDS and the other contractors.

Personnel responsible for administering the site will be kept abreast of current security practices to be able to effectively administer the ePN software.

Date:

To: Office of CIO

From: Kay Jacks, Designated Approving Authority

Subject: System Security Accreditation of [*System*]

A certification review of [*System*] has been conducted to determine its compliance with the Department's security requirements. Based on the results of the certification, and corrective actions implemented or planned to mitigate the risks associated with the identified vulnerabilities, we certify that [*System*] –

____ The application meets the documented and approved security requirements.

____ The application does not meet all documented and approved security requirements.

Weighing the requirements of [*System*] against residual risks, we recommend –

____ Full accreditation for initial/continued operation

____ Full accreditation for the initial or continued operation of the system contingent upon recommendations included in the certification evaluation report being implemented.

____ Initial accreditation for the initial or continued operation of the system contingent upon recommendations included in the certification evaluation report being implemented.

____ The application will not be accredited for initial or continued operations.

Certification of [*System*] at [*Location*] has been performed in accordance with OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," and the Department of Education Certification and Accreditation Program. The documented security requirements of [*System*] have been carefully reviewed and found to properly reflect controls required to protect the system and its information against unauthorized disclosure, alteration, or destruction.

A copy of this certification letter with supporting documentation generated during the certification shall be retained by the activity as a permanent record.

Signatures and Titles

APPENDIX A

STEP 1: Determine your Electronic Authentication Risk Category by documenting your response to each element.

Federal agencies shall assess overall risk and determine the appropriate electronic authentication technique in accordance with the following risk model. The three general factors used to determine the overall risk of transactions are risk of monetary loss, reputation risk, and productivity risk. After considering the components of the three risk factors found below, determine your system's risk category. For purposes of electronic transactions, there are four risk categories: high, moderate, low, and negligible.

In determining risk categories, Federal agencies should take into account programmatic controls, which mitigate the intrinsic risks of conducting transactions over an open network. (For example, a consumer who submits an Internet payment for goods in a Government auction may have to appear in person with identification to retrieve the goods. This may argue for a lower category of risk for the Internet transaction.)

Assess the combined risk factors (monetary loss, reputation risk, and productivity risk) to determine the risk category of your system.

(1) Determine your potential risk of monetary loss using a variety of elements, such as:

- (A) Average dollar value of transactions.
- (B) Loss to the Government.
- (C) Loss to a consumer.
- (D) Loss to a business, state or local government, or other trading partner.
- (E) Rules for reversing and repudiating a transaction (e.g., in the Uniform Commercial Code, the ACH rules, the Code of Federal Regulations, Federal Reserve regulations, Generally Accepted Accounting Principles, or bank network operating procedures).
- (F) Body of law applied to the transaction.
- (G) Liability for the transaction (e.g., personal, corporate, insured, or shared).

(2) Determine your potential reputation risk to the Government in the event of a breach or an improper transaction using elements such as:

- (A) Relationship with the trading partner (e.g., debiting a consumer account vs. intragovernmental payment between Federal agencies, and voluntary vs. mandatory transactions).
- (B) Public visibility and public perception of programs.
- (C) History or patterns of problems or abuses.
- (D) Consequences of a breach or improper transaction (e.g., normal exception handling vs. imposition of penalties).

(3) Determine your potential productivity risk associated with a breach or improper transaction using elements such as:

- (A) Time criticality of transactions (e.g., entitlement payment vs. contractor payment).
- (B) Scope of system and number of transactions (e.g., national or governmentwide system vs. localized system).
- (C) Number of system users or dependents.
- (D) Backup and recovery procedures.
- (E) Claims and dispute resolution procedures.

STEP 2: See if your type of electronic authentication (i.e. PIN) matches what is required for your risk category

The risk category indicates the robustness of the electronic authentication technique that must be used. Authentication rules for each of the risk categories are listed below. High and moderate risk transactions require multi-factor authentication, where at least two electronic authentication techniques must be used in combination, such as digital signature with a PIN protecting the signing key.

(1) High Risk

- (A) Multi-factor authentication is required, including a digital signature.
- (B) Private cryptographic keys must be generated, stored, and used in a secure cryptographic hardware module.
- (C) Certification authorities must operate under the Government's direct policy authority.

(2) Moderate Risk

- (A) Multi-factor authentication is required.
- (B) Private cryptographic keys may be stored in software.
- (C) Certification authorities, which are under the policy authority of a commercial entity meeting the requirements of this policy, may be used.

(3) Low Risk. Single factor authentication must be used, such as a PIN or a software based SSL client certificate.

(4) Negligible Risk. Transactions may occur without an electronic authentication technique.

STEP 3: Include your electronic authentication risk category in section 2.2 of the System Security Review.

APPENDIX B
CORRECTIVE ACTION PLAN

<i>NO</i>	<i>AREA</i>	<i>OBSERVATION</i>	<i>CORRECTIVE ACTION</i>	<i>STATUS</i>
1	Description of Information Sensitivity	There was no evidence of assigned values for the protection requirements (e.g., high, medium, low)	<p>The Department will work with the prime contractor in performing the following actions during future major software releases during the next calendar year:</p> <p>Classify data during the planning phase of each new implementation or upgrade of the February 2002-2003 release.</p> <p>Implement effective group controls for restricting access to data during the implementation of the February 2002-2003 release.</p> <p>Administer and monitor the system for compliance with the standard and restrictive access controls for the February 2002-2003 release.</p> <p>Compensating controls already exist which may have been overlooked by the Review team to include the use of specific group controls which restricts access to certain data. However, these controls take place later in the lifecycle.</p> <p>While we recognize that NIST is a guide and not necessarily a mandatory requirement, we believe the above actions provide a conservative approach in meeting the spirit and intent of A-130 standards in this area.</p>	
2	Rules of Behavior	There was no evidence that the Rules of Behavior are documented for DLOS.	<p>The Department has investigated this area with the prime contractor and observed that several compensating controls currently exist to include:</p> <p>The System Training Manual (latest version June 30, 2000) and the User Training Manual (latest version June 30, 2000) describe changes in system behavior, and provides the instructions for the use of the system by users.</p> <p>The Manual Procedures documentation (latest version September 29, 2000) as well as the Customer Service Representative (CSR) Manual (latest version March 31, 2000) describes how to answer phones, how to deal with customers for the CSRs, and the manual procedures for other departments, such as the mailroom.</p>	

<i>No</i>	<i>AREA</i>	<i>OBSERVATION</i>	<i>CORRECTIVE ACTION</i>	<i>STATUS</i>
			<p>CSR's and clerks are trained with each new release of the application on the use of the application, and how to deal with customers. Certain classified information, such as social security numbers, are shredded after it is used.</p> <p>Additionally, the Department will work with the prime contractor to enhance the Security Plan, to document policies and procedures regarding system set-up and maintenance, and the rules of behaviour for those using the system.</p> <p>Specifically, the Department will request that the plan be updated as follows:</p> <ul style="list-style-type: none"> Be enhanced to include further documentation regarding not only the responsibilities of the users within the system, but also the expected behavior of those individuals. Include details and set forth limits on the information sharing, which occurs between the LOS and other systems. Document the consequences that will occur if users or external vendors do not abide by the established policies and procedures. Include system installation procedures, which are not exempt from rules of behavior. Detail procedures for installing and administering Windows NT, both from System Administrator and Security Administrator points of view. <p>Additionally, we will investigate possibility of disseminating documentation of the policies and procedures (e.g. password policies, auditing procedures) surrounding the Windows NT environment to all appropriate users.</p>	
3	Security Lifecycle Planning	There was no evidence of appropriate security controls for each phase of the System Development Life Cycle.	<p>To validate compliance with NIST SP 800-18, the prime contractor's Documentation Manager was interviewed and it was noted that the Change Management manual documents, the controls in place to track changes to the system, including, using naming conventions. Furthermore, there is a change control process in place to</p> <p>Identify items that need to be changed</p>	

<i>No</i>	<i>AREA</i>	<i>OBSERVATION</i>	<i>CORRECTIVE ACTION</i>	<i>STATUS</i>
			<p>Control the changes for version control Track their status through the system Manage the data, and Perform audits to ensure that unauthorized changes do not occur. CCC/Harvest is being used for CM. Groups are used to control access to the Development environment. It is unclear, whether the Assessment team had access to or reviewed the compensating controls. We believe the current controls may satisfy the spirit and intent of the NIST guidance in this area. However, the Department will add additional support in this area by requesting written updates as necessary to the CM plan and SSP for future implementations and system upgrades with the security controls that are already in place.</p>	
4	Authorize Processing	<p>While this report and/or the operational/security controls reviews conducted in the past two (2) years could potentially serve as a basis for certification, there was no evidence that DLOS has sought certification or authority to operate.</p>	<p>In meeting the spirit and intent of A-130 guidance, the Department believes adequate authorization to operate has been given, as evidenced by the contract, task orders, and work orders which have been reviewed and awarded throughout the past several years. Thus, by authorization having been given for the system to process data, the associated risk has been accepted. It is also noted that FIPS 102 is not listed in the Statement of Work (SOW), Attachment 15, which lists the standards to which the prime contractor must adhere per its contract with the Department. In Attachment 15, FIPS 70 through 108 are listed as not applying to the contract. Therefore, FIPS 102 was excluded as a requirement. Although, we believe partial, if not full compliance has been met in this area and that a recertification is not necessary, a conservative position will be proposed to ensure the continuing relationship between the parties. Therefore, re-certification on a periodic (e.g., three years) basis will be investigated to ensure that the system maintains its</p>	

<i>No</i>	<i>AREA</i>	<i>OBSERVATION</i>	<i>CORRECTIVE ACTION</i>	<i>STATUS</i>
			<p>performance to the Department's standards. FIPS 102 may be used as the standard by which the re-certification may be conducted. Security gaps identified in the FIPS 102 testing will then be able to be bridged, and the Department will obtain a higher level of reliance that its systems are running securely. Additionally, security and risk concerns will be addressed during periodic PRR sessions prior the full implementation of each new release.</p>	
5	System Interconnection/Information Sharing	While interface specifications are reported to exist for all systems that are directly connected, there was no evidence of Memoranda of Understanding (MOU) or Trading Partner Agreements (TPAs)	<p>The system interconnection specifications are documented as Appendixes to the Task Orders. In addition, changes to the interface are documented as part of the minutes during interface meetings, which are published and archived in the shared directory. Specifications for the TIVWAN are published in the implementation guide that affects school-interfacing software, including Mainframe schools and Third-party software. Interface specifications between the LOS/CDS/DLSC are published as a read-only database, which can be provided. These specifications are validated in Intersystem Testing, Acceptance Testing, and First Live Batch Verification.</p> <p>It is the opinion of the Department that the system interconnections found in the aforementioned documents are sufficient to document interface specifications and compliance, therefore, no further action is needed to fulfill this part of the recommendation/observation. However, the Department may investigate the possibility of creating an MOU or TPA SFA-GAPS that may include information such as:</p> <ul style="list-style-type: none"> Roles and responsibilities Maintenance and making changes to the interfaces (or the systems in cases where the interface will be affected) Normal day-to-day activities. 	
6	Central Security Focus/Assigned		To investigate compliance with the A-130, the prime contractor's Security Administrator was interviewed. It was	

<i>No</i>	<i>AREA</i>	<i>OBSERVATION</i>	<i>CORRECTIVE ACTION</i>	<i>STATUS</i>
	Responsibility		<p>noted that training courses are documented and tracked in the system for each employee. Each employee's space on the system includes a "Training Plan" and a description of the courses the employee has taken. Hard copies of the EDS Security Administrator's training plan, course descriptions, and resume are attached. It was noted, however, that there was a lack of Windows NT-specific training listed in the Security Administrator's curriculum listing. We had identified this issue earlier via internal security audits conducted earlier this summer. The prime contractor is already addressing these concerns and the Department will monitor their corrective actions during the year.</p> <p>It was also noted that the Manual Procedures and User Guide provide guidance on how to use the LO application. These instructions supplement the external training that users undergo.</p> <p>As referenced above, it is the opinion of the Department that, in order to address the standards given by the A-130, in-depth Windows NT security training should be provided to the System Administrators and to the Security Administrator. This will allow these individuals to properly install, maintain, and secure the network. Additionally, to address the A-130, continuous "refresher" training programs should be provided to keep personnel abreast of the technological changes to the Windows NT operating system. By performing these actions, full compliance should be met as set forth in the A-130.</p>	
7	Applicable laws and regulations	DLOS is cognizant of applicable laws and regulations. Regarding the Privacy Act, DLOS has one system of records, however a System of Records Notice (SORN) has apparently not been submitted. Privacy Act data includes name, address, birth date, social security	The Department feels several compensating controls are in place, which satisfy the basic requirements in this area. The standard being referenced is NIST Special Pub 800-18, section 3.7.1, which states, in relevant part, that 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.	

<i>NO</i>	<i>AREA</i>	<i>OBSERVATION</i>	<i>CORRECTIVE ACTION</i>	<i>STATUS</i>
		<p>number, demographic, financial, statistical information and financial data. Information is retrieved by social security number (SSN). No alterations have been made to the system of records. DLOS has implemented and documented policies and procedures for access of records in accordance with Privacy Act requirements, but it is unclear from available evidence if similar policies and procedures exist for storage, retrieval, retention, and disposal. DLOS does not participate in any matching program with any other agency. There is no evidence that the contract with EDS requires contractors to comply with Privacy Act requirements.</p> <p>While training on security, including privacy act requirements, is supposed to be provided to all Department of Education employees and contractors annually, there was no evidence that DLOS personnel participate in such training. Disclosures of Privacy Act information are made by telephone to participating individuals or their authorized representatives in accordance with the system's published routine use. No logs of date, time, and content</p>	<p>Procedures for storage, retrieval, and retention of archived data are documented in the DRP and CM plans, as well as in the manual procedures. Per discussion with the EDS Security Administrator, on 4 October 2000, it was noted that all employees and contractors are required to complete a Privacy Act Statement and Declaration for Federal Employment (Optional Form 306, September 1994, US Office of Personnel Management) (both attached). The Declaration for Federal Employment includes a Privacy Act and Public Burden Statement. Procedures for disposal of sensitive information are documented in the SSP section 5.7.</p> <p>It was noted that the prime contractor performs archiving of production data. When the Department decides to close out a program year, the prime contractor performs balancing with the schools and Servicing. The Department gives authorization to perform archiving of old data on the system. Backups of data are created, and the database team archives the data through scripts. The process is changing to a form wherein an archive database is created that will hold specific portions of the data that is needed to satisfy requests from the Inspector General or the Department. No demographic (privacy act) data is removed from the loan system. Most of the data that is archived is loan and disbursement data. The Archive database has a higher level of restricted access than the Production database. The Archive database is held in a separate environment on the development server, which is a different machine than the area where the production data is held.</p> <p>While we feel basic requirements are being satisfied, the Department will discuss with the prime contractor the possibility of providing PA notices for customer service representatives in their work station handbooks.</p>	

<i>NO</i>	<i>AREA</i>	<i>OBSERVATION</i>	<i>CORRECTIVE ACTION</i>	<i>STATUS</i>
		of the phone calls are maintained. Applicants are given direct access to their data through this system. It is not clear how DLOS ensures that individual records are accurate through such mechanisms as editing software, software testing, or SFA testing and review. Only the institution of record can make changes to the data unless a request, in writing, is sent to the Loan Origination Center (LOC) for manual update by LOC personnel.		
8	Risk Management	While annual reviews and risk assessments are performed, the overall effectiveness level can be improved by EDS conducting consequence assessments and/or impact analysis, enhancing Disaster Recovery testing, proactively addressing findings including additional controls being initiated as applicable.		
9	Review of Security Controls	Processes are in place for reporting weakness and corrective actions. More emphasis and cooperation in responding to and ensuring effective remedial action in place across all sites would improve the overall level of effectiveness in this area. This is an on-going concern of the IQCU.		
10	Life Cycle	A strong software development life cycle exists as evidenced by recent		

<i>No</i>	<i>AREA</i>	<i>OBSERVATION</i>	<i>CORRECTIVE ACTION</i>	<i>STATUS</i>
		<p>SEI/CMM certification. This serves as a compensating control. However, it was not clearly evident that security resources and requirements were adequately addressed during all software releases. The IQCU sees this as a potential high-risk area since changes from major releases can impact the overall security of an IT system if not adequately addressed.</p>		
11	<p>Authorize Processing (Certification and Accreditation)</p>	<p>Compensating controls exist in the form of task orders, SOW, and other vehicles showing Department approval to authorize processing. Additionally, assessments conducted can serve as a foundation for formal certification. However, a formal re-certification or accreditation to meet the spirit and intent of the standard has not been accomplished within the past three years.</p>		
12	<p>System Security Plan</p>	<p>The current security plan and other supporting security documentation could be centralized to manage and implement security more effectively, and for easier access. Additionally, evidence from previous reviews shows the SSP at times has needed updating to meet current security standards. While evidence of recent updates was observed, improvement</p>		

<i>NO</i>	<i>AREA</i>	<i>OBSERVATION</i>	<i>CORRECTIVE ACTION</i>	<i>STATUS</i>
		opportunities exist in areas such as building maintenance documentation, network diagrams, etc.		
13	Personnel Security	Controls are in place and evident; previous reviews have shown the need for attention in updating screen access and segregation of duties. These remain IQCU concerns.		
14	Physical and Environmental Protection	Adequate physical security controls are in place along with off-site storage sites and procedures.		
15	Production, Input/Output Controls	Compensating controls are in place and tested which restrict access to sensitive data. However, internal/external labeling for sensitivity does not directly occur.		
16	Contingency Planning	DRP testing takes place annually along with tabletop simulations. Expanding scenarios to better test procedures for alternate site operations in the event of a natural disaster could enhance planning and testing.		
17	Hardware and System Software Maintenance	Solid SDLC is in place serving as a compensating control. Impact analysis should be considered.		
18	Data Integrity	No evidence of penetration testing performed; however, it is reported some penetration testing is conducted by a separate contractor who administers a portion of the LOS. IQCU recommends that		

<i>NO</i>	<i>AREA</i>	<i>OBSERVATION</i>	<i>CORRECTIVE ACTION</i>	<i>STATUS</i>
		penetration testing be considered along with enhanced use of intrusion detection tools as applicable.		
19	Documentation	As documented in previous reviews and responses to findings; compensating controls exist as evidence of good faith attempts and knowledge sharing. However, formal accreditation and written agreements between interconnected systems was not evident.		
20	Security Awareness, Training and Education	Mandatory annual refresher training is not being conducted.		
21	Incident Response Capability	Documentation describing procedures to follow for certain system security incident response mechanisms did exist; however, this documentation could be more comprehensive and management should ensure distribution to all users.		
22	Identification and Authentication	Stronger password controls are in place and evident as a result of EDS' response and corrective actions to earlier annual reviews and risk assessments from independent sources.		
23	Logical Access Controls	Logical access controls are in place. As noted in previous reviews, several areas of improvement exist which could enhance the level of effectiveness in this area.		
24	Audit Trails	Areas of improvement exist which could enhance the level of		

<i>NO</i>	<i>AREA</i>	<i>OBSERVATION</i>	<i>CORRECTIVE ACTION</i>	<i>STATUS</i>
.		could enhance the level of effectiveness in this area, such as creating a Systems and Security Administrator's Functions Validation list. This document could be used to assess the level of effectiveness as to whether technical security controls are being implemented and managed.		