

Loan Origination Subsystem (LOS) Corrective Action Plan

**Appendix B to ePN System Security Review
for June 28, 2001 Production Readiness Review**

No.	Area	Observation	Corrective Action	Status
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> <ul style="list-style-type: none"> • Classify data during the planning phase of each new implementation or upgrade of the February 2002-2003 release. • Implement effective group controls for restricting access to data during the implementation of the February 2002-2003 release. • Administer and monitor the system for compliance with the standard and restrictive access controls for the February 2002-2003 release. <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. 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> <ul style="list-style-type: none"> • 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. • The Manual Procedures documentation (latest version September 29, 2000) as well as the Customer Service 	

No.	Area	Observation	Corrective Action	Status
			<p>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> <ul style="list-style-type: none"> • 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>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. 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</p>	

No.	Area	Observation	Corrective Action	Status
			policies, auditing procedures) surrounding the Windows NT environment to all appropriate users.	
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> <ul style="list-style-type: none"> • Identify items that need to be changed • 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. <p>CCC/Harvest is being used for CM. Groups are used to control access to the Development environment.</p> <p>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	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	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	

No.	Area	Observation	Corrective Action	Status
		certification or authority to operate.	<p>associated risk has been accepted.</p> <p>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.</p> <p>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 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)	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.	

No.	Area	Observation	Corrective Action	Status
			<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 Responsibility		<p>To investigate compliance with the A-130, the prime contractor's Security Administrator was interviewed. It was 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</p>	

No.	Area	Observation	Corrective Action	Status
			<p>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	<p>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 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</p>	<p>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.</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</p>	

**Department of Education / EDS
 Loan Origination Subsystem
 Corrective Action Plan
 June 2001**

No.	Area	Observation	Corrective Action	Status
		<p>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 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.</p>	<p>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.</p> <p>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>	
8	Risk Management	<p>While annual reviews and risk assessments are performed, the overall effectiveness level can be improved by EDS conducting</p>		

Department of Education / EDS
Loan Origination Subsystem
Corrective Action Plan
June 2001

No.	Area	Observation	Corrective Action	Status
		<p>consequence assessments and/or impact analysis, enhancing Disaster Recovery testing, proactively addressing findings including additional controls being initiated as applicable.</p>		
9	Review of Security Controls	<p>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.</p>		
10	Life Cycle	<p>A strong software development life cycle exists as evidenced by recent 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	Authorize Processing (Certification and Accreditation)	<p>Compensating controls exist in the form of task orders, SOW, and other vehicles showing</p>		

**Department of Education / EDS
 Loan Origination Subsystem
 Corrective Action Plan
 June 2001**

No.	Area	Observation	Corrective Action	Status
		<p>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	System Security Plan	<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 opportunities exist in areas such as building maintenance documentation, network diagrams, etc.</p>		
13	Personnel Security	<p>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.</p>		

**Department of Education / EDS
Loan Origination Subsystem
Corrective Action Plan
June 2001**

No.	Area	Observation	Corrective Action	Status
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 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;		

**Department of Education / EDS
 Loan Origination Subsystem
 Corrective Action Plan
 June 2001**

No.	Area	Observation	Corrective Action	Status
		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 effectiveness in this area, such as		

**Department of Education / EDS
Loan Origination Subsystem
Corrective Action Plan
June 2001**

No.	Area	Observation	Corrective Action	Status
		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.		