

**Direct Loan Origination System (DLOS)
Corrective Action Plan,
September 2000**

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
1	Description of Information Sensitivity	There was no evidence of assigned values for the protection requirements (e.g., high, medium, low).		See the Recommendations relating to developing a security model below.		
2	Rules of Behavior	There was no evidence that the Rules of Behavior are documented for DLOS.		Document rules of behavior for DLOS. Ensure managers and users are trained to understand them.		
3	Security Life Cycle Planning	There was no evidence of appropriate security controls for each phase of the System Development Life Cycle.		Ensure that (as appropriate) privacy and security in the information life cycle are addressed in DLOS life cycle planning documents. See the Security Life Cycle Planning section for additional details		
4	Authorize Processing	While this report and/or the operational/security controls reviews conducted in the past two years could potentially serve as a basis for certification, there was no evidence that DLOS has sought certification or authority to operate.		Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal DLOS certification test under NIST guidance (FIPS 102).		
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).		Ensure all system connections and information sharing with non-SFA entities are codified in the DLSO security plan. See the section above on system interconnection and information sharing for further details.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
6	Central Security Focus/ Assigned Responsibility			<p>Ensure the CBS SSO is properly trained and qualified. See the section on security training and awareness, and the related recommendations for the Promote Awareness phase of the risk management cycle.</p> <p>In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.</p>		
7	Applicable Laws and Regulations	<p>DLOS is cognizant of applicable laws and regulations.</p> <p>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.</p> <p>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.</p> <p>DLOS does not participate in any matching program with any other agency.</p>		<p>Publish / update a DLOS SORN.</p> <p>Create/formalize policies and procedures for storage, retrieval, retention, and disposal of Privacy Act information.</p> <p>Ensure the contract with EDS requires contractors to comply with Privacy Act requirements.</p> <p>There was no evidence that DLOS personnel participate in annual Department of Education training on security and Privacy Act requirements.</p>		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		<p>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.</p> <p>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>				