

**Postsecondary Education Participants Systems (PEPS)  
Corrective Action Plan,  
September 2000**

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
1	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 PEPS life cycle planning documents. See the Security Life Cycle Planning section for additional details.		
2	Application Software Maintenance Controls	There was no evidence of controls for the maintenance of the application.		Examine ED guidance relating to system life cycle planning. Ensure that PEPS CM processes and procedures are consistent with that guidance, and that the PEPS SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.		
3	Data Integrity / Validation Controls	There was no evidence of controls for assuring the integrity and validity of the data.		Ensure PEPS complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details.		
4	Security Awareness and Training	<p>There was no evidence of policies or procedures for implementing a security awareness program.</p> <p>Security awareness training has not been implemented for the school and GA user community.</p>		Provide security training for the PEPS SSO; once trained, the PEPS SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
5	Authorize Processing	Although PEPS has not sought certification, this report could serve as the basis for a system certification/ 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 PEPS certification test under NIST guidance (FIPS 102).		
6	Central Security Focus/ Assigned Responsibility	Data ownership has not been defined clearly.		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. 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.		
7	Audit Trails	Auditing on the HP/UX is disabled.  Auditing on the Oracle RDBMS is disabled.		Ensure PEPS audit results are being used effectively to help PEPS managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
8	Identification and Authentication	<p>There was no evidence of policies for defining the password management process, or procedures for monitoring it.</p> <p>The minimum user password length for the Oracle and ReachOut systems is significantly shorter than the industry standard six-character.</p> <p>PEPS user initial passwords are defaulted to UserIDs, which are known to all PEPS users.</p> <p>Oracle and ReachOut systems allow trivial passwords.</p> <p>The Oracle, HP/UX, and ReachOut systems do not force the users to change their passwords periodically.</p> <p>The convention for assigning PEPS user initial passwords is stated in the PEPS System Security Plan.</p>		<p>Ensure PEPS complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.</p>		
9	Logical Access Controls	<p>There was no evidence of policies for defining the logical access control process, or procedures for monitoring it.</p> <p>Oracle users are given unlimited invalid logon attempts by rebooting their workstations.</p> <p>Terminated employee access or employees who no longer need access to PEPS aren't removed from system.</p>		<p>Document and implement within one year PEPS-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.</p>		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
10	Production, Input / Output Controls	There was no evidence of controls for the installation and use of the application.		Implement Security Life Cycle Planning, Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the PEPS security plan.		
11	System Interconnection / Information Sharing	There was no evidence of Memoranda of Understanding (MOU), or Trading Partner Agreements (TPA), or that the interfaces had been addressed in the Security Plan.		Ensure all PEPS connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.		
12	Applicable Laws and Regulations	PEPS is cognizant of applicable laws and regulations. The status of Privacy Act compliance is unknown. Although this system presumably complies with notice, publication, and annual/biennial/quadrennial review requirements, as those remain the responsibility of the Department's Chief Privacy Officer, no system-specific information with regard to access controls, storage, retrieval, retention, disclosure logging, contractor compliance, disposal of records, or employee training was provided for these systems.		N/A		