

**Central Processing System (CPS)
Corrective Action Plan,
September 2000**

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
1	Risk Assessment and Management	No risk assessment has been performed for CPS.		Implement the GAO risk management cycle in the CPS environment. See the other improvement suggestions for this system as well as the Conclusions and Recommendations sections.		
2	Security Life Cycle Planning	There was no evidence of appropriate security controls for each phase of the System Development Life Cycle.		Ensure (as appropriate) privacy and security in the information life cycle are addressed in CPS life cycle planning documents. See the Security Life Cycle Planning section for additional details.		
3	Security Awareness and Training	There was no evidence of policies or procedures for implementing a security awareness program. Security awareness training has not been implemented.		Provide security training for the CPS SSO; once trained, the CPS 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.		
4	Rules of Behavior	Rules of behavior for CPS are not documented in detail.		Document rules of behavior for CPS. Ensure that managers and users are trained to understand them.		
5	Authorize Processing	Although CPS 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 CPS certification test under NIST guidance (FIPS 102).		
6	System Interconnection/ Information Sharing	There was no evidence identifying whether or not CPS interfaces with other SFA systems or external entities.		Ensure all CPS connections and information sharing with non-SFA entities are codified. 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
7	Data Integrity / Validation Controls	There was no evidence of controls for assuring the integrity and validity of the data.		Ensure CPS complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details		
8	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 CPS CM processes and procedures are consistent with that guidance, and that the CPS 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.		
9	Identification and Authentication	There was no evidence of policies for defining the password management process or procedures for monitoring it. TIVWAN passwords are stored in clear text (uncompressed) on two occasions during the password change process. FAFSA employees have access to a password database. Passwords are not as strong as good business practices warrant.		Ensure CPS complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
10	Logical Access Controls	<p>There was no evidence of policies for defining the logical access control process, or procedures for monitoring it.</p> <p>RACF's automatic account revocation capability may not be activated.</p> <p>Unsecured E-Mail used for requesting new CPS accounts.</p> <p>The ACSO has no active role in user account management.</p> <p>Sensitive information contained in documentation or other media is not identified clearly with an external label or other markings.</p> <p>No log-on banner alerts users their actions may be monitored.</p> <p>Although the ACSO participates in the CPS CM process, this participation is in capacities other than security.</p>		Document and implement within one year CPS-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.		
11	Documentation	There is no current and approved CPS security plan.		Develop a NIST-compliant (Special Pub 800-18) security plan for CPS. See the Recommendations section for additional details.		
12	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 CPS security plan.		
13	Contingency Planning	<p>The ACSO did not have a copy of the contingency plan.</p> <p>The ACSO did not have a copy of the disaster recovery plan.</p> <p>NCS has no formal procedures for dealing with security incidents.</p>		Ensure formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the CPS SSO has a copy of all plans.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
14	Audit Trails	The Department does not review audit logs. NCS does not provide quarterly reports of extracted audit data.		Ensure CPS audit results are being used effectively to help CPS managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.		
15	Central Security Focus / Assigned Responsibility	The ACSO position is not a full-time position. The ACSO and OPE CSO are not always kept informed of security issues that may affect their systems or their operations. The ACSO has no contact with the contractor security personnel. The CPS COTR performs many of the ACSO functions. The ACSO has not received technical security training.		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.		
16	Applicable Laws and Regulations	CPS 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		