

**Campus Based System (CBS)
Corrective Action Plan,
September 2000**

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
1	Security Awareness and Training	While CBS reports they are aware of ED security training requirements, they do not report actually attending it. This is of particular concern for the CBS SSO, who is new to his position and does not have a security background.		Provide security training for the CBS SSO; once trained, the CBS 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.		
2	Security Life Cycle Planning	CBS has no security plan, and management reports that life cycle security planning is largely "Not Applicable" despite the high requirement for data integrity.		Ensure that security in the information life cycle is addressed in CBS life cycle planning documents. See the Security Life Cycle Planning section for additional details.		
3	Rules of Behavior	Rules of Behavior for CBS do not exist.		Document rules of behavior for CBS. Ensure managers and users are trained to understand them.		
4	Data Integrity/Validation Controls	There was no evidence of controls for assuring the integrity and validity of the data.		Ensure CBS complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details		
5	Production, Input/Output Controls	CBS reports production controls are not required or do not exist.		Implement Security Life Cycle Planning, Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the CBS security plan.		
6	System Interconnection / Information Sharing	CBS does not have MOUs or MOAs that govern its connection to TIVWAN.		Ensure all CBS connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.		
7	Authorize Processing	Although CBS has not sought certification, this report or the 1998 BAH A-130 report could serve as the		Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO. perform a formal CBS		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		basis for a system certification/authority to operate.		certification test under NIST guidance (FIPS 102).		
8	Identification and Authentication	<p>The standard is currently being met partially. CBS features some automated password standard enforcement, but several limitations were reported.</p> <p>Passwords lengths as short as 4 characters are allowed; 6 character should be the minimum.</p> <p>Passwords are currently alpha characters only; numbers and special characters should be allowed.</p> <p>There is currently no restriction on the frequency of change; this allows users to easily bypass the 3-generation password history.</p> <p>Passwords should have a minimum time limit of 30 days.</p>		Ensure CBS complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.		
9	Logical Access Controls	<p>At the application level CBS has a simple individual-based access control matrix; access options are read-only, read/update, or administrator (all access). These permissions are associated with individual user IDs and protected by a password dialogue. Network access is controlled by the TIVWAN and EDNET authorities, not by CBS management.</p> <p>Nonetheless, several limitations were noted over and above the password standards concerns noted above. These include:</p> <ul style="list-style-type: none"> • There was no evidence of policies for defining the logical access 		Document and implement within one year CBS-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		<p>control process, or procedures for monitoring it</p> <ul style="list-style-type: none"> • There are no lockouts and logouts when a user leaves a terminal • No log-on banner alerts users that their actions may be monitored <p>In addition, there was no evidence that concerns from previous risk assessments and control reviews had been addressed. These include:</p> <ul style="list-style-type: none"> • RACF's automatic account revocation capability is not activated • There are no special protections assigned to the Default Reduction Assistance Program (DRAP) database • Protect-all option has not been activated • Batchallracf has not been activated • Tape data set protection has not been activated • All users have Time Sharing Option (TSO) access 				
10	Documentation	<p>The standard is currently being met partially. While CBS does maintain some software/application documentation, functional requirements, and system test results, many other required documents are missing. These include:</p> <ul style="list-style-type: none"> • vendor hardware documentation • major application security plan • standard operating procedures 		<p>Develop a NIST-compliant (Special Pub 800-18) security plan for CBS. See the Recommendations section for additional details.</p>		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		<ul style="list-style-type: none"> • emergency procedures • contingency plans • user rules/procedures • risk assessment • certification/accreditation statements/documents 				