

**Recipient Financial Management System (RFMS)  
Corrective Action Plan,  
September 2000**

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
1	Audit Trails	<p>There was no evidence that procedures were in place to review audit trails.</p> <p>No ongoing effort to ensure there is a complete audit trail that records user activity.</p> <p>The "Protectall" feature of RACF is not activated. This would provide default protection for datasets and other general resources.</p> <p>Seven program names have the privilege to bypass RACF password authorization checking, per the DS-MON report.</p> <p>The RACF audit function is not used to track the activities of selected (privileged) users.</p>		<p>Ensure Pell audit results are being used effectively to help Pell managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.</p>		
2	Security Awareness and Training	<p>References were made to documents that were not included with the document under review.</p> <p>Security awareness and training are especially important given the maintenance and development environment.</p> <p>Contractors on-site at ED have not received any specific security training or refresher awareness briefings.</p> <p>The ED Functional System</p>		<p>Provide security training for the Pell SSO; once trained, the Pell 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.</p>		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		<p>Manager has received no systems security training.</p> <p>There is not formal security awareness program with the RFMS, OPE, or SFA.</p> <p>RFMS management is satisfied with the level of security awareness; however, they also stated that it could be improved.</p>				
3	Security Life Cycle Planning	<p>There was no evidence of appropriate security controls for the Maintenance, Disposal, and Authorization phases of the System Development Life Cycle.</p>		<p>Ensure privacy and security in the information life cycle are addressed in Pell life cycle planning documents. See the Security Life Cycle Planning section for additional details.</p>		
4	System Interconnection/ Information Sharing	<p>There was no evidence that the interfaces had been addressed in the Security, Internal Controls, and Auditability Plan.</p>		<p>Ensure all Pell connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.</p>		
5	Authorize Processing	<p>Although Pell has not sought certification recently, this report could serve as the basis for a system certification/ authority to operate.</p> <p>Prior to this security review, Pell had not been certified or granted approval to operate by a DAA within the last five years.</p>		<p>Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal Pell certification test under NIST guidance (FIPS 102).</p>		
6	Personnel Security	<p>Incomplete security forms provided by ACS has caused delays in initiating the background screening for contract employees.</p> <p>Security is not specifically</p>		<p>Implement ED personnel security guidance. See the Personnel Security section for additional details.</p>		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		mentioned in key ED personnel position. ACS has received no official notification of the results of any of the background screenings.				
7	Production, Input/Output Controls	References were made to documents that were not included with the document under review. Status of the production and input/output controls is unknown to the reviewers as the environment and contractors have changed since the last review.		Implement Security Life Cycle Planning, Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the Pell security plan.		
8	Contingency Planning	Continuity of operations planning (for users) and disaster recovery planning for portions of RFMS run at ACS are not complete. These plans need to address critical dependence on key staff as a potential point of failure. ED participated in the establishment of an incident response capability that made available the resources of the NASA Computer Incident Response Capability (NACIRC). This incident response capability was not funded and is no longer available. ACS controls and procedures for computer incident response are not formally documented.		Ensure formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the Pell SSO has a copy of all plans.		
9	Application Software	There was no evidence that		Examine ED guidance relating to system		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
	Maintenance Controls	<p>procedures are in place to protect against illegal use of software.</p> <p>No separate test environment exists.</p> <p>Testing is not performed in a rigorous manner.</p> <p>Once PRC lost the follow-on contract, there was difficulty in getting PRC staff to meet contract requirements.</p> <p>The RFMS production and test environments are mixed.</p> <p>ACS used a unlock/rename/lock process to manage program changes.</p> <p>Lack of a true test environment is a concern.</p> <p>Production access can eliminate/bypass the librarian control.</p> <p>Undue reliance on a single individual for continued operation of the RFMS.</p> <p>Timely ED approval for production changes is a concern.</p> <p>Growing number of overrides pointing to libraries considered developmental.</p>		<p>life cycle planning. Ensure that Pell CM processes and procedures are consistent with that guidance, and that the Pell 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.</p>		
10	Data Integrity / Validation Controls	<p>Integrity and availability are the primary concerns for RFMS. Related to these concerns are members CDSPS01, CDSPS03, CDSPA17, CDSPA02, and CDSPA24. Those with "S" in the</p>		<p>Ensure Pell complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details.</p>		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		5th position are the most unreliable and those with "A" in the 5th position can cause the most damage to RFMS.				
11	Documentation	The Security Plan does not meet the requirements of the Computer Security Act of 1987, and OMB 90-08. RFMS application documentation is not current and ACS staff are not at all satisfied with the system documentation that exists.		Develop a NIST-compliant (Special Pub 800-18) security plan for Pell. See the Recommendations section for additional details.		
12	Identification and Authentication	No password dictionary checking is performed to prevent users from choosing easily-guessed passwords (common passwords). The amount of time it takes to receive a user ID after submission of the ITS form 88-01 seems longer than necessary.		Ensure Pell complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.		
13	Logical Access Controls	Production programs are supposed to run from the production library, which is a protected library. Overrides have been requested to allow production programs to run from the development library. No other controls over dialing in, such as restricting incoming calls to those from modem pools or those with dial-back are used. Lockheed-Martin staff were directed by ED to maintain the existing rules that PRC created		Document and implement within one year Pell-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>and have been following the previously-defined RACF rules. The lack of defined policies and procedures has increased the difficulty of day-to-day operations as well as routine tasks.</p>				
14	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 relating to 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>		