

Security Action Decision Memorandum

<u>System Information</u>	
System Owner:	Jennifer Douglas
System Manager:	
Supporting Contractor:	
System Tier:	
System Criticality:	
Data Sensitivity:	
Confidentiality:	
Integrity:	
Availability:	

Requirements

OMB Circular A-130 requires Federal organizations to certify and accredit all General Support Systems and Major Applications. ED/OCIO's Information Security policy, as well as FSA's Information Technology Security and Privacy policy, reinforces this federal requirement.

As part of its FISMA reporting, the Department's Deputy Secretary informed OMB that Education will certify and accredit all tier three and four systems by December 31, 2003. The Deputy Secretary provides quarterly progress updates to OMB.

ED Schedule – Events – Reporting

ED/OCIO maintains a security-related action item list for the all Department systems.

The relevant dates for FSA are as follows:

Configuration Management Plan	February 28, 2003
System Security Plan-	May 5, 2003
COS/DR Plans-	May 5, 2003
Risk Assessment	
Remediation completed	May 5, 2003
NIST Self-Assessment	May 30, 2003
Revalidate CIP Questionnaire and	
Inventory Worksheet	June 30, 2003
Security Testing and	
Evaluation Plans	August 4, 2003
C&A package	September 15, 2003

Security Action Decision Memorandum

Reason(s) for System Retirement

[Describe the rationale for retiring the system and replacing it.]

Retirement Plan

[Describe overall plan to retire system, including final retirement date]

Security Action Decision Memorandum

Cost Breakdown		
[Assess the costs to complete/update each item in the list below]		
	Actual	FSA Estimate (Medium-sized system)
System Security Plan	\$	\$75 K
Disaster Recovery Plan	\$	\$30 K
Continuity of Support Plan	\$	\$30 K
Configuration Management Plan	\$	\$40 K
POA&M remediation	\$	See estimates in POA&M
C&A package, including ST&E Plan	\$	\$30 K
C&A testing	\$	\$100 K*
C&A remediation	\$	Determined by test results

*Funding source unknown (Department or POC)

FSA Security Perspective

Certification and Accreditation (C&A) reassures system managers, owners and auditors that appropriate security controls were designed, tested and implemented properly. C&A formalizes the security risk management approach used by managers to assess the robustness of their information systems. C&A is not a paper drill or a security exercise that should be thought of as an action item to be checked off of a list. Rather, system managers should use C&A to identify system weaknesses and address egregious vulnerabilities. System Owners may choose to accept the risk resulting from the C&A analysis, transfer the risk (insurance), or reduce their risk through mitigation actions.

Federal and Department requirements do not provide security exemptions for systems still in operation. Operational systems remain vulnerable to threats, both internal and external. C&A will lessen the risk of system compromise. System Owners must weigh the costs vs. risks for each security action taken or not taken.

FSA Business Perspective

[Describe business reasons for completing/not completing certification and accreditation]