

# **Security Requirements and Test Procedure Review Workshop**

## **March 25-26, 2003**

### **Overview**

The Certification and Accreditation process is a requirements evaluation. It is a process that management uses to evaluate its system ('s) compliance with Federal and Departmental regulations and stated security requirements. Compliance can be measured a number of ways, either by interview, observation, test, or documentation review. The depth and breadth of the testing is constrained by available resources (budget and people), time available for certification testing, and a "reasonableness" concept based on the relative criticality of the systems to be certified. The Department of Education is a civilian agency that does not process classified data, does not maintain national security systems, but does process Privacy Act and financial data. Therefore, certification testing should be performed at a reasonable level consistent with the sensitivity of the data the Department must protect.

### **Workshop Objectives**

The two-day security requirements and test procedure review workshop will review the test requirements and associated test procedures created from a finite list of Federal and Department regulations, security requirements, and guidance documents. The documents are:

- ED BLSR
- ED CAPP
- ED CIPP
- ED CPG
- ED GSS/MA IP
- ED IT CMP
- ED IT SCP
- ED IT SP
- ED IT SPMP
- ED SDLCG

And for FSA

- FSA IT SPP
- FSA SSLCG

We will rely on Xacta/Telos' existing test procedures for Federal documents such as 800-26, OMB A-130, etc.

### **Workshop Procedures**

The members of the Workshop group, from ED OCIO and FSA CIO, will use a standard methodology to evaluate each security requirement and test procedure. The criteria are:

- Does the security requirement make sense and it is phrased clearly?
- Does the test methodology (I, O, T, D) make sense for a tier 3 or 4 system?
- Does the test procedure make sense and will it allow the CRG to validate the effective operation of the security control?

For each security requirement, the workshop group will annotate recommended changes and updates to any of the criteria noted above.

The result of the workshop will be an agreed upon list of requirements and test procedures that OCIO will require the CRG to execute once each ED system completes its individual security test and evaluation plan.