Functional Series 500 **INTERIM UPDATE 08-04**
Management Services

SUBJECT: Revision of ADS 545, Information System Security

NEW MATERIAL: ADS Chapter 545, Information System Security, has been updated to address two specific issues. The first is to address the difference between electronic and digital signatures and the second is to align ADS policy with OMB guidance.

EFFECTIVE DATE: 04/30/2008

POLICY

USAID/General Notice
M/CIO & M/CIO/CISO
04/30/2008

Subject: Revision of ADS 545, Information System Security

ADS Chapter 545, Information System Security, has been updated to address two specific issues. The first is to address the difference between electronic and digital signatures and the second is to align ADS policy with OMB guidance.

Here are the changes:

545.3.5.23 Electronic Signatures

An electronic signature is an electronic signal, sound, symbol, or process executed or adopted by an authenticated and authorized individual, with the intent to sign an electronic record, document or file (for submission or approval), and which is unique to the individual and under his or her sole control, and bound to the electronic record, document or file within a system. The following policies apply to the use of electronic signatures within USAID.

- The Chief Information Security Officer (CISO) must establish procedures for the use of electronic signatures within USAID systems.

545.3.5.24 Digital Signatures

A digital signature is produced by two mathematically linked cryptographic keys, a private key used to sign, and a public key used to validate the signature. A digital signature is created when a person uses his or her private key to create a unique mark on an electronic document. The recipient of the document employs the person's public key to validate the authenticity of the digital signature and to verify that the document was not altered subsequent to signing. Digital signatures are often used within the context of a Public Key Infrastructure (PKI) in which a trusted third party known as a Certification Authority (CA) binds individuals to private keys.

- The CISO may establish procedures for the use of digital signatures within USAID.

Additionally, to clarify a supplemental policy originally issued to address Office of Management and Budget (OMB) Memorandum 06-16, the CISO is replacing "cannot" with "may" and "must" with "should generally," as shown below. These changes conform USAID policy with OMB's currently interpretation for certain systems which contain limited amounts of personally identifiable information.

- 545.3.1.4(b) During the design phase of their system, the System Owner must conduct a security categorization of the information to be processed by their systems, and include the details of this categorization in the System Security Plan. System Owners may categorize systems that process personally identifiable information as "low"--they should generally be categorized as at least "moderate."

Point of Contact: Any questions concerning this Notice may be directed to Rhonda Turnbow, M/CIO/CISO, (202) 712-0106.

Notice 04131

File Name	IU5_0804_050708
Notice Date	04/30/2008
Effective Date	04/30/2008
Editorial Revision Date	
ADS CD No.	N/A
Remarks	This IU will remain active on the ADS Web site for three months.