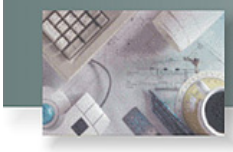

Compliance Component

DEFINITION	
Name	Cryptography Design/Implementation
Description	Cryptography Design and Implementation considerations include: • Hardware v. Software Encryption • Encryption Key Management • Cryptography Export Rules
Rationale	A responsible authority in each organization should ensure that their information systems that utilize cryptography provide an acceptable level of security for the given application and environment. Determine the following: • Platform to be used (i.e. mainframe, server, client, appliance) • Usage (i.e. stored data encryption, data transmission, message authentication, digital signature) • Interdependencies with physical security, user authentication, audit trails, etc • Level of data protection needed (laws, regulations, policies) • Procedures for secure installation, generation, and start-up of a cryptographic module. • Procedures for maintaining security while distributing and delivering versions of a cryptographic module to authorized operators. • Correspondence between the design of the hardware, software, and firmware components of a cryptographic module and the cryptographic module rules of operation.
Benefits	• Provide a common level of security and interoperability among users. By using accepted standards, organizations can reduce costs and protect their investments in technology. • Provide solutions that have been accepted by a wide community, and that have been reviewed by experts in relevant areas. Standards help ensure interoperability among different vendors' equipment.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Cryptography
List Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL			
State the Guideline, Standard or Legislation	See sub-components of Cryptography Design and Implementation considerations: • Hardware v. Software Encryption • Encryption Key Management • Cryptography Export Rules		
Document Source Reference #	(All found at www.csrc.nist.gov) NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook (Oct 1997) NIST SP 800-21, Guideline for Implementing Cryptography in the Federal Government (Nov 1999) NIST SP 800-45, Guidelines on Electronic Mail Security (Sep 2002) NIST Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules (May 2001)		
Standard Organization			
Name	NIST Federal Information Processing Standards	*Website*	www.csrc.nist.gov/publications/fips/index.html
Contact Information	inquiries@nist.gov		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	www.csrc.nist.gov/publications/fips/index.html
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords			
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		

AUDIT TRAIL			
Creation Date	04/13/2004	*Date Accepted / Rejected*	4/13/04
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			