COMPLIANCE COMPONENT

DEFINITION	
Name	Acquisition and Development Phase
Description	The system life cycle security Acquisition and Development Phase is a process to establish and document security requirements, and incorporate them into an information system.
Rationale	Agencies must consider information security in all phases of information systems management. The inclusion of security early in the information System Development Life Cycle (SDLC) should result in a less expensive and more effective system than adding security features at a later time.
Benefits	• Including security at the beginning of the SDLC provides for a better protected system • Incorporating comprehensive security measures for a system is usually less expensive than the cost of recovering from a security incident

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Management Controls
Specify the Technology Area Name	System Life Cycle Security
Specify the Product Component Name	

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

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	Agencies must establish and document security requirements for information systems in the Acquisition and Development phase. This is accomplished by performing a security requirements analysis commensurate with the size and complexity of the system. The requirements analysis draws on and further develops the work performed during the Initiation phase. Components of the security requirements analysis are: • **Risk Assessment** – a formal process that identifies high impact assets, potential threats, and recommended controls. This builds on the initial risk assessment performed during the Initiation phase, but will be more in-depth and specific. It is used to determine what types of controls will be cost effective and will form the basis for determining mandatory and desirable security specifications for the developing system. • **Security Functional Requirements Analysis** – analysis of requirements that may include the following components: o State and agency information security policies

	o state security architecture o laws, regulations, agreements (MOUs) • **Security Assurance Requirements Analysis** – analysis of requirements for assurance that the system information security will work correctly and effectively. o ensures security functional requirements that have been identified are sufficiently detailed and are testable (e.g. system security controls) o used as the basis for determining how much and what kinds of compliance are required (e.g. accreditation, certification, third-party evaluation, testing) • **Cost Considerations** – cost/benefits of security features must be considered in requirements analysis. • **Security Planning Documentation** – ensures security controls, planned or in place, are fully documented.
Document Source Reference #	NIST SP 800-64 Rev. 2, Security Considerations in the Information System Development Life Cycle; FIPS 199, Standards for Security Categorization of Federal Information and Information Systems; FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

Compliance Sources			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name		*Website*	
Contact Information			

KEYWORDS	
List Keywords	Requirements, SDLC, risk, impact, threat, controls, policy, architecture, laws, regulations, agreements, assurance, cost, compliance, assessment, analysis

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				

CURRENT STATUS				
Provide the Current Status	☐ *In Development*	☐ *Under Review*	☒ *Approved*	☐ *Rejected*

AUDIT TRAIL			
Creation Date	08/03/2006	*Date Approved / Rejected*	04/26/2018
Reason for Rejection			
Last Date Reviewed	04/26/2018	*Last Date Updated*	04/26/2018
Reason for Update	Vitality		