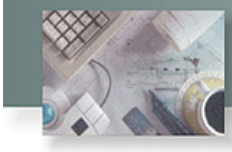

Compliance Component

DEFINITION	
Name	Cyber Security Technical Training
Description	Cyber Security Technical Training is a formalized process necessary for agencies' security specialists to secure the information, hardware and software.
Rationale	Cyber Security Technical Training is needed so that an agency's security specialists can adequately protect an agency's information and information resources.
Benefits	• Provides the tools necessary to develop and implement security processes.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Operational Controls
List the Technology Area Name	Security Awareness Training and Education
List Product Component Name	

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

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	To be considered a security technician one must have an understanding and working knowledge of security principles and a comprehensive knowledge of their technical field. To keep pace with technology, the IT security body of knowledge is vast and growing at an accelerated rate. However, there are fundamental IT security concepts that establish a foundation for technical training and education. In addition to a comprehensive knowledge of their technical field, a working knowledge of the following is also necessary: • Laws and regulations • IT security program • System environment • System interconnection • Information sharing • Risk Management • Life Cycle controls

	• Management controls • Operational controls • Technical controls • Handling sensitive and classified information Cyber Security Technical Training includes formal courses and certification programs such as: • Operating Systems • Applications • Protocols • Security tools • Technical controls • Policy and procedures • Risk Assessment • Security Plans • Networks		
Document Source Reference #	NIST Special Publication 800-16 – Information Technology Security Training Requirements: A Role- and Performance-Based Model NIST Special Publication 800-50 – Building an Information Technology Security Awareness and Training Program		
Standard Organization			
Name		*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
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	2/8/2007	*Date Accepted / Rejected*	03/23/2007
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			