COMPLIANCE COMPONENT

DEFINITION	
Name	Strong Authentication
Description	Strong Authentication is the requirement to use multiple factors to verify the identity of a user accessing networks and/or applications, as opposed to the typical method which requires only one factor of authentication.
Rationale	Strong authentication provides additional assurance that the user is who they say they are and the data they send to you is authentic.
Benefits	Strong authentication counters the weaknesses inherent in typical, one-factor authentication methods because they are: • Harder to duplicate, • Cannot be re-generated, • Cannot be easily guessed, • Cannot be re-used, or are • Physically stored independently from the other factor of authentication, thereby deterring simultaneous use by an unauthorized user. Strong authentication increases the feasibility of using single sign-on (SSO).

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Technical Controls
Specify the Technology Area Name	Identification/Authentication
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	The three factors of authentication for users are: 1. Something they know, for example: • Password • Personal Identification Number (PIN) • Personal Question (such as your favorite color) 2. Something they have, for example: • Token • Certificate • Smartcard • Magnetic Stripe/Credit/Debit Card • One-time Pad

	• Proximity Card 3. Something they are, for example: • Fingerprint • Retinal Scan • Voice Scan • Facial Scan Strong Authentication must use at least two <u>different</u> factors from the list above. For example, one password they know plus one token they have. It must <u>not</u> use two of the same type of factor, for instance, a password and a personal question. Cookies are not an acceptable authentication factor. Strong Authentication must be implemented when: • Users access the private network from public connections, such as the Internet • Applications perform transactions involving CONFIDENTIAL or financial information via the Internet • Administrators remotely manage security devices • Password policies cannot be enforced Strong Authentication should be implemented when: • CONFIDENTIAL information is accessed within the internal network • Administrators remotely manage servers and network devices Strong Authentication methods must lock the user account, and require administrator intervention or a waiting period of at least 30 minutes, after a minimum of 3 failed authentication attempts.
Document Source Reference #	NIST 800-63B, *Digital Identity Guidelines: Authentication and Management.* June 2017.

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	Password, One-Time, Token, Certificate, Bio-Metric, Smartcard, advanced authentication, two-factor, Single Sign On, SSO, cookies, transaction, PIN

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

COMPONENT SUB-CLASSIFICATION		
Sub-Classification	Date	Additional Sub-Classification Information
☐ *Technology Watch*		
☐ *Variance*		
☐ *Conditional Use*		

Rationale for Component Classification	
Document the Rationale for Component Classification	

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	05/12/05	*Date Approved / Rejected*	09-27-2005
Reason for Rejection			
Last Date Reviewed	1-23-2020	*Last Date Updated*	1-23-2020
Reason for Update			