COMPLIANCE COMPONENT

DEFINITION	
Name	Cryptography for Web Servers
Description	Cryptography for Web Servers provides authentication and encrypts the data in transit.
Rationale	Cryptography provides the necessary security features to protect the data on web servers that are unsecure.
Benefits	• Server authentication • Client authentication • Data integrity • Confidentiality • User authentication

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Technology Controls
Specify the Technology Area Name	Cryptography
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 most commonly used encryption protocol is Secure Socket Layer (SSL). HTTPS is Hypertext Transport Protocol integrated with SSL. SSL is sometimes referred to as SSL/TLS (Secure Socket Layer/Transport Layer Security).
	
	• When transmitting sensitive or critical information over the web, users shall use SSL with at least:
	  ○ Advanced Encryption Standard (AES) 256-bit encryption
	  ○ Secure Hash Algorithim-2 (SHA-2)
	  ○ Transport Layer Security v 1.2 (TLS v 1.2)

Document Source Reference #	NIST Special Publications 800-52, Rev. 2 – Guidelines for the Selection, Configuration and use of Transport Layer Security (TLS) Implementations; IRS Publication 1075

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

	(CSRC), IRS		
Contact Information	inquiries@nist.gov		
Name		*Website*	
Contact Information			

KEYWORDS

List Keywords	SSL, HTTPS, FTP, SMTP, AES, Digital Signature, SHA-2,TLS, Cryptography, Web Server

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	10/27/2016	*Date Approved / Rejected*	10/27/2016
Reason for Rejection			
Last Date Reviewed	03/13/2023	*Last Date Updated*	03/16/2023
Reason for Update	Vitality		