COMPLIANCE COMPONENT

DEFINITION

Name	Virtual Private Network (VPN)
Description	A Virtual Private Network (VPN) can be a software or hardware network technology that creates a secure encrypted network connection over a public network to an agency's network.
Rationale	A Virtual Private Network (VPN) provides a low-cost means of establishing a secure private connection for remotely accessing an agency's private network.
Benefits	• Provide opportunities for increased productivity of mobile employees, telecommuters, business partners and remote sites by allowing access to agency resources • Provides for the confidentiality and integrity of the agency's data in transit across the public network • More cost effective than alternatives such as dedicated private telecommunications lines between agencies or branch offices

ASSOCIATED ARCHITECTURE LEVELS

Specify the Domain Name	Security
Specify the Discipline Name	Technical Controls
Specify the Technology Area Name	Remote Access Controls
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Standard
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	• VPNs must meet the Cryptography for VPNs Compliance Component (CC) requirements • VPNs must meet applicable requirements in the Securing Remote Computers and Connections CC • An anomaly-identifying software or hardware (Intrusion Detection and Prevention System) should be in place inside the point in the agency network where VPN traffic is decrypted (see the Intrusion Prevention System IPS CC) • Site-to-Site VPNs: o A VPN uses dedicated equipment and strong encryption to secure point to point communications over a public network.

- Must authenticate the tunnel with a:
  - Pre-shared key or
  - certificate
- May utilize Access Control Lists (ACLs) on the VPN device to limit what resources can be accessed
- Must not allow split-tunneling unless an agency-controlled firewall is properly positioned between the agency network and any non-agency or public network (see the Firewall Environments CC)

  NOTE: Split tunneling occurs when concurrent access is allowed to resources on the agency network and a non-agency or public network via the VPN

- Remote Access VPNs:
  - Remote Access VPN is a client-to-LAN connection by users who need to securely connect to the agency network from remote locations. This can be via wireless, Digital Subscriber Line (DSL), cable modem, etc.
  - Must authenticate the VPN tunnel with a:
    - Two-Factor authentication (NIST SP 800-63-1)
  - Must not allow split tunneling (only one network connection is allowed)
  - Should utilize Access Control Lists (ACLs) to limit what resources can be accessed by a remote client (see Access Control Lists CC)

Document Source Reference #	NIST Special Publication 800-46 v2, SP 800-114, SP 800-47, SP 800-77, SP 800-113

Compliance Sources

Name	National Institute of Standards and Technology (NIST)	*Website*	http://csrc.nist.gov
Contact Information	info@nist.gov		
Name		*Website*	
Contact Information			

Keywords

List Keywords	Broadband, Cable, DSL, Wireless, Satellite, Modem, Internet, Dial-Up, telecommute, mobile, remote, IPSec, tunnel, site-to-site

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	10/04/2016	*Date Approved / Rejected*	10/04/2016
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	10/04/2016
Reason for Update	Vitality		