



COMPLIANCE COMPONENT

DEFINITION	
<i>Name</i>	Securing Remote Computers and Connections
<i>Description</i>	<p>Securing Remote Computers and Connections is the means used to ensure the confidentiality, integrity and availability of agency information transmitted via unsecured connection.</p> <p>Remote access includes, but is not limited to:</p> <ul style="list-style-type: none"> • DSL • Cable • Wireless • Satellite • ISDN • Dial-up
<i>Rationale</i>	Computers not attached to a private network pose a higher risk of data breach. Proper security configuration is needed to reduce the risk of transmitting agency data via an unsecured connection.
<i>Benefits</i>	<ul style="list-style-type: none"> • Expands the means of securely transmitting agency data via an unsecured network connection.
ASSOCIATED ARCHITECTURE LEVELS	
<i>Specify the Domain Name</i>	Security
<i>Specify the Discipline Name</i>	Technical Controls
<i>Specify the Technology Area Name</i>	Remote Access Controls
<i>Specify the Product Component Name</i>	
COMPLIANCE COMPONENT TYPE	
<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	
COMPLIANCE DETAIL	
<i>State the Guideline, Standard or Legislation</i>	<p><u>Securing Remote Computers</u></p> <ul style="list-style-type: none"> • Only agency-approved equipment may be remotely connected to the agency network • Virus protection software must be installed and kept current on remote systems • Computers connected to the agency network shall not simultaneously connect to any other network via another network device, i.e., internal modem, external modem, Network Interface Card (NIC), wireless NIC, split-tunneling etc. • Operating systems must be kept up-to-date on remote computers per agency requirements • Remote computers must be disconnected from the network when not in

	<p>use</p> <p><u>Securing Remote Connections</u></p> <ul style="list-style-type: none"> • Agency approval is required before any user may connect remotely to the agency network • Remote connections must meet the cryptography compliance component requirements (see Cryptography for VPN and Cryptography for Web Servers) • Remote connections used for transmitting agency information must meet the Advanced/Strong Authentication compliance component. 		
<i>Document Source Reference #</i>	NIST Special Publication 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.		
Compliance Sources			
<i>Name</i>	NIST, CERT@Coordination Center	<i>Website</i>	csrc.nist.gov, www.cert.org
<i>Contact Information</i>			
<i>Name</i>		<i>Website</i>	
<i>Contact Information</i>			
KEYWORDS			
<i>List Keywords</i>	Broadband, Cable, Digital Subscriber Line (DSL), Wireless, Satellite, Modem, Internet, Virtual Private Network (VPN), Dial-Up, Bring Your Own Device (BYOD), Remote Access, Telework, Telecommute		
COMPONENT CLASSIFICATION			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i> <input checked="" type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>		
<i>Sunset Date</i>			
COMPONENT SUB-CLASSIFICATION			
Sub-Classification	Date	Additional Sub-Classification Information	
<input type="checkbox"/> <i>Technology Watch</i>			
<input type="checkbox"/> <i>Variance</i>			
<input type="checkbox"/> <i>Conditional Use</i>			
Rationale for Component Classification			
<i>Document the Rationale for Component Classification</i>			
Migration Strategy			
<i>Document the Migration Strategy</i>			
Impact Position Statement			
<i>Document the Position Statement on Impact</i>			
CURRENT STATUS			
<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i> <input type="checkbox"/> <i>Under Review</i> <input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>		
AUDIT TRAIL			
<i>Creation Date</i>	10/27/2016	<i>Date Approved / Rejected</i>	10/27/2016

<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	10/27/2016
<i>Reason for Update</i>	Clarified for simultaneous network connections		