Compliance Component

DEFINITION	
Name	Security for Voice Over Internet Protocol (VOIP)
Description	Security for Voice Over Internet Protocol (VOIP) refers to securing IP networks when transmitting voice across them.
Rationale	Transmitting voice over data networks increases the complexity and vulnerability of the networks. Although VOIP is widespread, the technology is often incorrectly implemented, and often lacks compatibility and continuity with existing systems. This can lead to compromised security.
Benefits	• Securing VOIP transmissions ensures the confidentiality, integrity, and availability of both voice and data communications
ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Remote Access Controls
List Product Component Name	
COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	
COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	• Agencies must perform a risk assessment before deploying VOIP systems. o The assessment must examine and ensure the agency can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations. • The agency network infrastructure and security, including firewalls, IDSs, VPNs, etc., shall be capable of supporting VOIP. • Sufficient backup power shall be available for the office VOIP switch, if the VOIP function is critical. • Agencies must ensure that adequate physical security is in place to restrict access to VOIP network components. o This will deter insertion of sniffers or other network monitoring devices as well as physical damage. • Agencies must use a mechanism to allow only authorized VOIP traffic through firewalls. o A variety of protocol dependent and independent solutions

  - are available, including stateful firewalls that understand VOIP, application level gateways (ALGs) for VOIP protocols, Session Border Controllers, or other standards-based solutions when they mature.

Gateway Management

- Strong authentication (see the Advanced/Strong Authentication Compliance Component) and access control must be used for administrators on voice gateway systems.
- IPsec or Secure Shell (SSH) must be used for all remote management and auditing access.
  - It is preferable to do VOIP gateway management from a physically secure system.

Softphones

- "Softphone" systems shall not be used over a public network or connection, even if the voice conversation is not confidential, because it creates more avenues of attack into the data network.

  The only exception is that softphones may be used over a public network if the connection is via VPN without split-tunneling.
  - A softphone is software and the communication system internal to the PC to replicate a standard telephone handset or deskset.
  - Softphones do not work in a separated VLAN configuration.
- Any remote access services, such as FTP and Telnet, shall be disabled on the laptop, workstation or PDA, as well as any local administration and management features for the local user.

Desksets

- When agencies use VOIP desksets, they must separate voice and data on logically different networks (VLANs). This includes separate address blocks used for voice and data traffic.
  - Separate VLANs allows for proper configuration of firewall and intrusion detection systems, as well as making it easier to provide Quality of Service (QOS).
- Any remote access features on the VOIP desksets, such as FTP and Telnet, shall be disabled as well as any local administration and management features.
- A voice gateway which interfaces with the Public Switched Telephone Network (PSTN) must not allow the H.323 protocol, Session Initiation Protocol (SIP), or other VOIP protocols on the data network.
- Default login and administrator passwords on VOIP phones shall be changed from the default.

Remote IP Phones

	- Mobile units integrated with the VOIP system must use products implementing WiFi Protected Access (WPA) or 802.11i Robust Security Network (RSN) encryption. - Default login and administrator passwords on VOIP phones shall be changed from the default. Public Networks - Encryption is required when transmitting confidential or trusted information over a public network, such as the Internet. - Encryption must be done from end to end, which may negatively impact performance.		
Document Source Reference #	NIST Special Publication 800-58, Security Considerations for Voice Over IP Systems (Jan 2005) www.csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf		
Standard Organization			
Name		*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	www.csrc.nist.gov/publications/fips/index.html
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords	Softphone, Telephony, IPT, H.323, PSTN, SIP, PBX, POTS, ALGs, WPA, RSN, VoIP, encrypt, deskset, phone		
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		*Date Accepted / Rejected*	05/10/2005
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			