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	
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	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	• Agencies must perform a risk assessment before deploying VOIP systems and as dictated by state or federal requirements. 　　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.

- 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.

- Softphone systems shall only be used over a private network if the user is not working with FTI, PII, etc.

- Any remote access services, such as FTP and Telnet, shall be disabled on the laptop, workstation or mobile device, 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.

- 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.
	<u>Public and Private Networks</u>
	• Encryption is required when transmitting confidential or trusted information over a public network, such as the Internet.
	• Encryption may be required when transmitting confidential or trusted information over a private network, depending on the agency.
	• 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

Compliance Sources

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		
Name		*Website*	
Contact Information			

KEYWORDS

List 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*
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	05/10/2005	*Date Approved / Rejected*	02/10/2023
Reason for Rejection			
Last Date Reviewed	02/02/2023	*Last Date Updated*	02/10/2023
Reason for Update			